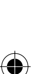
1/2008

Datenschutz Nachrichten

31. Jahrgang
ISSN 0137-7767
9,00 Euro

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de



Datensschutz an Hochschulen

Datenschutz und Datensicherheit an Hochschulen ■ „Ich habe nichts zu verbergen“ ■ Lehrevaluation ■ E-Learning-Systeme ■ StudiVZ ■ geplante Visa-Warndatei ■ Datenschutznachrichten ■ Rechtsprechung ■ Buchbesprechungen ■ Presseerklärungen ■



Autoren dieser Ausgabe:

Dr. Heiner Bielefeldt
Direktor des Deutschen Instituts für Menschenrechte, Berlin
bielefeldt@institut-fuer-menschenrechte.de

Sören Jungjohann
Assessor jur., Hannover
soeren.jungjohann@web.de

Dr. Kai-Uwe Loser
Mitarbeiter beim Datenschutzbeauftragten der Ruhr-Universität Bochum
kai-uwe.loser@rub.de

Ingrid Pahlen-Brandt
Datenschutzbeauftragte der Freien Universität Berlin
pahlen@zedat.fu-berlin.de

Martin Rost
Mitarbeiter beim Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein, Kiel
martin.rost@web.de

Peter Schaar
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bonn
poststelle@bfdi.bund.de

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, Kiel
weichert@datenschutzzentrum.de

Prof. Dr. Michael Wettern
Datenschutzbeauftragter Technische Universität Braunschweig
datenschutz@tu-braunschweig.de

Termine

Mittwoch, 4. Juni 2008
Arbeitnehmer-Datenschutz aktuell
Datenschutz-Fachtagung 2008, BTQ Niedersachsen, in Hannover
weitere Informationen siehe unter www.btq.de

Donnerstag, 5. Juni 2008
Datenschutzgerechter Umgang mit Studierendendaten
Universität Stuttgart (Campus Stadtmitte)
weitere Informationen unter www.zendas.de

Sonntag, 20. Juli 2008
DVD-Vorstandssitzung in Bonn
(Interessierte DVD-Mitglieder mögen sich bitte bei der Geschäftsstelle melden.)

Mittwoch, 8. Oktober 2008
Datenschutz bei E-Learning-Plattformen
Universität Stuttgart (Campus Stadtmitte)
weitere Informationen siehe unter www.zendas.de

Donnerstag/Freitag, 9./10. Oktober 2008
2. Fachtagung für Datenschutzbeauftragte an Hochschulen und anderen wissenschaftlichen Einrichtungen
Freie Universität Berlin, weitere Informationen unter www.datenschutz.fu-berlin.de

Sonntag, 12. Oktober 2008
DVD-Vorstandssitzung in Frankfurt
(Interessierte DVD-Mitglieder mögen sich bitte bei der Geschäftsstelle melden.)

Freitag, 24. Oktober 2008
Verleihung der Big Brother Awards
Bielefeld, weitere Informationen unter www.bigbrotheraward.de

Dienstag, 9. Dezember 2008
Datenschutz in Forschung und Lehre - Technische Aspekte
Universität Stuttgart (Campus Stadtmitte)
weitere Informationen unter www.zendas.de



DANA
Datenschutz Nachrichten
ISSN 0137-7767
31. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Bonner Talweg 33-35, 53113 Bonn
Tel. 0228-222498
E-Mail: dvd@datenschutzverein.de
www.datenschutz.de

Redaktion (ViSdP)
Hajo Köppen
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Bonner Talweg 33-35, 53113 Bonn
dana@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Sascha Hammel,
35398 Gießen
Hammelwood@web.de

Druck
Wienands Printmedien GmbH
Linzer Str. 140, 53604 Bad Honnef
wienandsprintmedien@t-online.de
Tel. 02224 989878-0
Fax 02224 989878-8

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für Mitglieder ist der Bezug kostenlos.
Ältere Ausgaben der DANA können teilweise noch in der Geschäftsstelle der DVD bestellt werden.

Copyright
Die Urheber- und Vervielfältigungsrechte liegen bei den Autoren. Der Nachdruck ist nach Genehmigung durch die Redaktion bei Zusendung von zwei Belegexemplaren nicht nur gesattet, sondern durchaus erwünscht, wenn auf die DANA als Quelle hingewiesen wird.

Leserbriefe
Leserbriefe sind erwünscht, deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Titelbild: Frans Jozef Valenta
Rückseite: unbekannt



Berlin ist eine Reise wert…….

Hochschulen sind in zweifacher Hinsicht mit dem Datenschutz betraut. In Lehre und Forschung sind Datenschutz und IuK-Technologien Gegenstand von Lehrveranstaltungen und Entwicklungsprojekten. Gleichzeitig sind Hochschulen Verarbeiter personenbezogener Daten. Über 1,9 Millionen Studierende sind zur Zeit an den deutschen Hochschulen immatrikuliert; die Zahl der Beschäftigten liegt bei rund 275.000. Der Einsatz von automatisierten Personalverwaltungs-, Arbeitszeiterfassungs-, Immatrikulations-, Prüfungs-, Evaluations- und Haushaltsverwaltungssystemen etc. ist heute an der kleinsten Hochschule Standard. Chipkarten, eLearning-Angebote und Online-Verfahren für unterschiedlichste Anwendungen kommen vermehrt zum Einsatz.

Angesichts der hohen Dichte von IuK-Systemen und der daraus resultierenden Datenschutzfragen und –probleme verwundert es, dass Hochschulen eher selten unter Datenschutz- und Datensicherheitsaspekten betrachtet werden. Die „1. Fachtagung für Datenschutzbeauftragte an Hochschulen und anderen wissenschaftlichen Einrichtungen" im September 2007 an der FU Berlin schuf die Möglichkeit zum bundesweiten Austausch über aktuelle Datenschutzthemen an Hochschulen. Die DANA will mit der Veröffentlichung der Tagungsreferate einen Beitrag zur Vernetzung der Datenschützer an Hochschulen leisten. Und jetzt schon auf die 2. Fachtagung am 9./10. Oktober 2008 neugierig machen.

Hajo Köppen

Inhalt

Ingrid Pahlen-Brandt

Erste Fachtagung für Datenschutzbeauftragte von Hochschulen und anderen wissenschaftlichen Einrichtungen 2007 an der Freien Universität Berlin DATENSCHUTZ – SICHER FÜR FREIHEIT

Vorgeschichte

Bei meiner Datenschutzarbeit an der Freien Universität Berlin wurden und werden mir noch immer die Verhältnisse an anderen Hochschulen als Argument gegen datenschutzrechtliche Forderungen entgegengehalten. Was an anderen Hochschulen möglich und üblich sei, müsse doch auch an der Freien Universität Berlin erlaubt sein. Die prominentesten Beispiele für diese Argumentation sind die Einführung der Telefonanlage im Jahre 2001, der Versuch der HIS POS Einführung in den Jahren 2001 bis 2004 sowie aus jüngster Zeit die Wahl zu den DFG Fachkollegien 2007.



- Bei der Einführung der Telefonanlage stellte sich als Problem die datenschutzgemäße Speicherung der Verbindungsdaten. Der Hinweis auf die bisherige eigene Praxis und die anderer Einrichtungen erschwerten die Entscheidung für die erforderliche ergänzende Programmierung der HICOM- Anlage durch Siemens. Nach den Zusatzarbeiten war die HICOM-Anlage das einzige Produkt, das die gesetzlichen Anforderungen Berlins technisch abbilden konnte.[1]

- Bei der Bearbeitung der datenschutz rechtichen Fragen im Zusammenhang mit der versuchten Einführung von HIS POS, einer Software zur Unterstützung der Prüfungsverwaltung, wurde wiederholt auf den massenhaften Einsatz von HIS-Produkten an deutschen Hochschulen verweisen.

  Ein Beispiel aus jüngster Vergangenheit: Für die Wahlen zu den Fachkollegien sollten als Bestandteil der Wahlprotokolle personenbezogene Daten übermittelt werden. Die DFG ging davon aus, dass die von den einzelnen Wahlstellen in den Mitgliedseinrichtungen zuzuordnenden Nummern der Wahlunterlagen zu den einzelnen Wählern keinen Personenbezug hätten. Wenn Daten nicht als personenbezogen angesehen werden, sind die datenschutzrechtlichen Bestimmungen für den Umgang mit ihnen nicht einzuhalten.

So reifte während der vergangenen Jahre der Wunsch nach einem unmittelbaren Austausch mit den Datenschutzkollegen. So wie für die Mitglieder der allgemeinen Hochschulverwaltung und der Rechenzentren üblich - z.B. die Kanzlertagungen - ist es auch für den Datenschutz sinnvoll, die besten Lösungen für die eigene Institution in Diskussionen mit den Kollegen zu finden.

Durchführung

Neben den Datenschutzbeauftragten als Teilnehmer der Tagung wurden die anderen wissenschaftlichen Einrichtungen einbezogen. Soweit die Datenschutzarbeit Verwaltung und Wissenschaft betrifft, gleichen sich die zu bearbeitenden Fragen. In allen diesen Einrichtungen sind die Grundrechte der Wissenschaftsfreiheit und der informationellen Selbstbestimmung abzuwägen.

Um einer Zusammenarbeit mit anderen wissenschaftlichen Institutionen näher zu kommen, lud ich zum 13./14. September 2007 zur Ersten Fachtagung für Datenschutzbeauftragte an Hochschulen und anderen wissenschaftlichen Einrichtungen in der Bundesrepublik an der Freien Universität Berlin unter dem Titel „DATENSCHUTZ - SICHER FÜR FEIHEIT“.

Peter Schaar, der Herr Bundesbeauftragte für den Datenschutz und die Informationsfreiheit übernahm die Schirmherrschaft über die Tagung und betonte hiermit die Bedeutung des Datenschutzes an Hochschulen. In seinem Grußwort, dass er nach der Begrüßung durch die Erste Vizepräsidentin der Freien Universität Berlin an die Teilnehmer richtete, wies er auf die wichtige gestaltende Aufgabe der Datenschutzbeauftragten hin.

Teilgenommen haben circa 100 Datenschutzbeauftragte und andere am Datenschutz Interessierte. Neben Datenschutzbeauftragten kamen Mitglieder von Personalvertretungen, Mitarbeiter aus Hochschulrechenzentren sowie auch ein studentischer Vertreter. Fünf Landesdatenschutz-beauftragte schickten Mitarbeiter und auch Firmen, die Datenschutz als Dienstleistung anbieten, waren vertreten. Die Teilnehmer waren aus der gesamten Bundesrepublik angereist, lediglich das Bundesland Thüringen war nicht vertreten.

Der Leitgedanke bei der Auswahl der Themen war ihre Praxisrelevanz; die Beiträge sollten den Teilnehmern für die Alltagspraxis relevante Themen zur Diskussion stellen.

Für den einleitenden Beitrag des Leiters des Instituts für Menschenrechte, **Heiner Bielefeldt**, gilt dies in besonderem Maße. Sein Beitrag, *Freiheit und Sicherheit im Demokratischen Rechtsstaat*, vermit-

1 Pahlen-Brandt, „Datenschutzgerechte Speicherung von Verbindungsdaten an der Freien Universität Berlin, SPLITTER Nr. 3/2001 S. 39 auch http://www.itdz-berlin.de/dokumentation/splitter/splitter_2001_3.pdf.

telte die Bedeutung des Datenschutzes für eine demokratische Gesellschaft freier Bürger. Zu oft wird der Wert des Datenschutzes im Alltag in Frage gestellt, so dass es sinnvoll erschien, dieses Thema offen anzugehen und Hilfe hieraus für die notwendigen Diskussionen zu schöpfen. Der Beitrag von Bielefeldt bildet gleichsam ein Fundament für die Datenschutztätigkeit.

Das weitere Hauptthema bildete die für die Gestaltung datenschutzgemäßer IT-Verfahren erforderliche Regelungskompetenz in den Ein-richtungen. Datenschutzgemäß ist ein Verfahren nur dann, wenn rechtliche, technische und organisatorische Aspekte in geeigneter Weise zusammenspielen. Dieses Ziel bei komplexen IT-Verfahren zu erreichen, erfordert Fachkunde auf allen Gebieten und ist sinnvoll zu erreichen nur bei der Einbeziehung der Datenschutzaspekte von Anfang an. Nach Beiträgen zu einzelnen Aspekten anhand von aktuellen Verfahren an Hochschulen bildete hier der Beitrag von **Martin Rost** vom Landeszentrum für Datenschutz in Schleswig-Holstein „*Datenschutzaudit an Hochschulen, Methode und Erfahrungen aus Schleswig-Holstein*“ einen Überblick über diese komplexen Vorgänge. In seinem Beitrag führte er aus, dass Datenschutzarbeit zugleich wertvolle Managementberatung für die Institutionen sein kann, wenn nur datenschutzgemäße Verfahren Ziel der Einführung eines Verfahrens ist. In diesem Zusatznutzen des Datenschutzes erkennt er eine Erklärung für die steigende Nachfrage nach Datenschutz-Audits in Schleswig-Holstein.

Sowohl **Kai-Uwe Loser**, Ruhruniversität Bochum, in seinem Beitrag „*E-.Learning: Regelungsbedarfe und Technikentwicklungen zwischen informationeller Selbstbestimmung und Freiheit der Lehre*“ mit vielen technischen Aspekten als auch **Michael Wettern**, Datenschutzbeauftragter der Technische Universität Braunschweig, in seinem Beitrag „*Lehrevaluation an Hochschulen*“ erkannten gravierenden Nachholbedarf für den Erlass von Satzungen. Die Hochschulen versäumen oft den Erlass von Satzungen, so dass in großem Maße an deutschen Hochschulen Personendaten ohne ausreichende Erlaubnisregelung verarbeitet werden. Dass die Verarbeitung der Personendaten damit rechtswidrig ist, ist offensichtlich in der Regel für die Leitungen der Hochschulen nicht beunruhigend.

Die Datenschutzbeauftragten haben als „zahnlose Papiertiger“ selbst in Fällen offensichtlichen Verstoßes gegen das Gesetz keine Möglichkeiten, aus eigenen Rechten als Datenschutzbeauftragte datenschutzgemäße Zustände zu bewirken. Die insoweit unzureichende Umsetzung der EG-Datenschutzrichtlinie führt so auch an Hochschulen zu fortwährender massenhafter Rechtsverletzung, denn den Datenschutzbeauftragten in der Bundesrepublik sind keine wirksamen Einwirkungsbefugnisse verliehen, so wie es Artikel 28 Abs. 2 zweiter Spiegelstrich der EG-Datenschutzrichtlinie fordert, wenn mit der Bestellung von Datenschutzbeauftragten Erleichterungen bezüglich der Meldeerfordernisse verbunden sein sollen.[2]

Der Beitrag „*Infrastruktur zur verteilten Authentifizierung und Autorisierung mit Shibboleth im Rahmen der Deutschen Föderation DFN-AAI*“ von **Ato Ruppert** von der Universitätsbibliothek Freiburg entwickelte Verfahren zu datensparsamer Rechteverwaltung in einer Konföderation, die vom DFN-Verein zukünftig in der deutschen Wissenschaftslandschaft angeboten werden wird. Mitglieder einer Hochschule können auch von anderen Orten aus die ihnen über die Hochschule vermittelte Rechte nutzen. Die Berechtigungsprüfung erfolgt an der Heimateinrichtung, an den die Anfrage vom Diensteanbieter übermittelt wird. Der Diensteanbieter braucht so keine Kenntnis von Personendaten, er verlässt sich auf das OK der Heimateinrichtung.

Andreas Lang, Universität Magdeburg, präsentierte die Arbeit von Jana Dittmann, Andreas Lang, Tobias Scheidat und Claus Vielhauer „*Aspekte des Datenschutzes beim Umgang mit multi-modalen biometrischen Daten im Forschungsumfeld!*“ [3].

2 Pahlen-Brandt, Sind Datenschutzbeauftragte zahnlose Papiertiger?, DuD 2007, 24ff. sowie: Mehr Kompetenzen für den Datenschutzbeauftragten, DuD 2003, 637ff.

3 Innovationsmotor IT-Sicherheit 10. Tg-Band Dt. IT-Sicherheitskongress des BSI 2007.

Am Anfang der abschließenden Podiumsdiskussion[4] führte **Lorenz Hilty**, von der Empa[5] aus St. Gallen, in den aktuellen Stand der Entwicklung der RFID-Anwendungen ein. In der Podiumsdiskussion wurde unter lebhafter Beteiligung der Zuhörer erörtert, wie der Datenschutz an wissenschaftlichen Einrichtungen und in der Gesellschaft insgesamt einen besseren Stand erreichen kann.

Ausblick

Dem Ziele der Tagung entsprechend - Kontakt zwischen den Daten-schutzbeauftragten zu fördern - wurden Gespräche unter den Teilnehmern bereits bei der Programmgestaltung berücksichtigt. Die zur Verfügung stehende Zeit wurde rege genutzt und viele Kontakte geknüpft. In der Folge der Veranstaltung wurde eine bundesweite Mailingliste für Datenschutzbeauftragte eröffnet, die durchaus Beachtung findet. Ein Wiki zum Datenschutz an wissenschaftlichen Einrichtungen ist geplant und kommt hoffentlich bald in Gange.

2008 wird es eine weitere Tagung geben. Im Mittelpunkt dieser Tagung sollen die rechtlichen Aspekte des Datenschutzes stehen, die - dies zeigte bereits die erste Tagung - oft unzureichend sind oder sogar gänzlich fehlen. Die Tagung soll auch Raum bieten für die Frage, ob und ggf. welche Folgerungen sich für den Datenschutz daraus ableiten lassen, dass Verstöße ohne Irritation geradezu als unerheblich betrachtet werden: Zeigt dies, dass der Datenschutz veraltet ist oder ist das Konzept zu abstrakt, um sich in der Praxis bewähren zu können oder sind es andere Mängel?

Es wird vieles für den Datenschutz erreicht sein, wenn er beim Ranking von Hochschulen berücksichtigt wird. Die Handhabung des Datenschutzes an anderen Hochschulen ist untauglich als Argument für ein Festhalten an schlechten Lösungen. Ziel muss ein Wettstreit um gute Datenschutzpraxis zwischen den Hochschulen sein.

4 Weitere Teilnehmer der Podiumsdiskussion waren Bielefeldt, Rost, Loser, Diskussionsleitung Pahlen-Brandt.

5 Eidgenössische Materialprüfungs- und Forschungsanstalt.



Peter Schaar

Grußwort zur Ersten Fachtagung für Datenschutzbeauftragte an Hochschulen und anderen wissenschaftlichen Einrichtungen

Sehr geehrte Damen und Herren, seit den ersten Datenschutzgesetzen der 70er und frühen 80er Jahre des inzwischen vergangenen Jahrhunderts haben die Herausforderungen beim Schutz der Privatsphäre beständig zugenommen. Die moderne Kommunikations- und Informationsgesellschaft ist von der allgegenwärtigen Verarbeitung personenbezogener Daten und den vielfältigen Möglichkeiten der Vernetzung derselben geprägt. Seitdem Kunden- und Kreditkarten unsere Portemonnaies verstopfen, wir täglich online einkaufen, chatten und ein Profil auf einer der unzähligen Onlineplattformen zu hinterlegen längst zum guten Ton gehört, scheint die Vorstellung eines Rechts auf informationelle Selbstbestimmung, also einer Kontrolle darüber, was Dritte über einen selbst wissen, fast anachronistisch zu sein. Fast beiläufig entstehen heute ständig neue Nutzer- und Nutzungsdaten, durch die wir bewertet und kategorisiert werden – etwa in gute und schlechte Kunden. Öffentliche Räume werden immer flächendeckender videoüberwacht, der Anpassungsdruck an das sozial erwünschte Verhalten steigt so ständig, die Digitalisierung weiter Lebensbereiche prägt immer mehr unsere Umwelt.



Die große Herausforderung des Datenschutzes wird es sein, diese Vernetzungsmöglichkeiten in Bahnen zu lenken, die – bei allen Vorteilen und Bequemlichkeiten – Raum lassen nicht nur für die bloß unbeobachtete Privatsphäre, sondern für die freie und manchmal auch unangepasste Selbstentfaltung des einzelnen Menschen.

Diese datenschutzrechtliche Entwicklung betrifft die Hochschulen und Forschungseinrichtungen gleich in mehrfacher Hinsicht: sie sind als Nutznießer, aber auch Verpflichtete der gesetzlichen Regelungen gefordert. Sie sind zudem als Vordenker und Initiatoren für neue Wege im Datenschutzrecht angesprochen. Denn Hochschulen und Forschungseinrichtungen sind von jeher Experimentierfelder technischer und gesellschaftlicher Entwicklung gewesen. Forschung und Lehre sind nicht zuletzt deshalb frei und durch das Grundgesetz geschützt, um Wege abseits der eingetrampelten Pfade gehen zu können. Trotzdem bedarf es auf diesen neuen Wegen Wegweiser und Leitplanken, und der Datenschutz, die Achtung vor der Privatsphäre des Einzelnen, ist eine davon.

Im Mittelpunkt wissenschaftlicher Tätigkeit steht der Umgang mit Informationen. Daten – personenbe-zogene und nicht personenbezogene – bilden dafür den Rohstoff. Andererseits braucht der Datenschutz das Fachwissen und die Neugier der Hochschulen und Forschungseinrichtungen als Denkwerkstätten, um die Auswirkungen der zunehmenden Digitalisierung auf den Menschen und das menschliche Zusammenleben zu erfassen. Forscher haben eine besondere Verantwortung, denn bei Forschungsvorhaben gilt es nicht nur den Forschern einen optimalen Zugang zu den erwünschten und erforderlichen Daten zu verschaffen, sondern auch die Rechte der Betroffenen auf informationelle Selbstbestimmung zu gewährleisten. Die Freiheit von Forschung und Lehre darf nicht auf Kosten der Datensicherheit und des Datenschutzes gehen. Umgekehrt setze ich mich dafür ein, dass wir Datenschützer nicht nur sagen, was nicht geht, sondern uns an der Suche nach Wegen beteiligen, die fundierte und kreative Forschung unter Wahrung von Persönlichkeitsrechten ermöglicht und gewährleistet.

Forschungsvorhaben, die gezielt personenbezogene Daten sammeln, beschäftigen sich häufig mit besonders sensiblen und daher besonders schützenswerten Daten. Fragen zur Religion, zum Gesundheitszustand, über Vorlieben und Neigungen sind nicht nur für den Forscher interessant, sondern wecken die Neugier vieler Dritter, vor allem im Hinblick auf ihre kommerzielle Verwertbarkeit. Umso wichtiger ist es, bereits beim Forschungsdesign kreativ zu sein und dabei auch das Recht auf informationelle Selbstbestimmung zu berücksichtigen, etwa durch frühzeitige Anonymisierung und die Nutzung pseudonymer Daten. Auch bei der Präsentation von Forschungsergebnissen muss die Privatsphäre der Beteiligten geschützt bleiben. Die jeweiligen Forschungsvorhaben müssen immer wieder anhand dieser Prämissen kritisch überprüft werden. In der Zusammenarbeit mit den Landesbeauftragten wird hier zum Teil erhebiche Arbeit betrieben, um zu einem vernünftigen und für beide Seiten befriedigenden Ausgleich zu kommen. Datenschutz leistet hier einen Beitrag zur ethischen Forschung und steigert damit ihre gesellschaftliche Akzeptanz.

Fragen des Datenschutzes betreffen Hochschulen auch in ihrer Rolle als Datensammler über die Menschen, die in ihnen wirken und arbeiten. Immer wieder in der Diskussion sind die Datensammlungen über Studierende. Studierendenausweise werden mit immer mehr Funktionen versehen, enthalten damit immer mehr Daten. Trotz aller Bequemlichkeit und Vorteile, die solche Systeme bieten, darf die Transparenz für die Betroffenen nicht vernachlässigt werden. Außerdem wecken Datensammlungen immer auch Begehrlichkeiten und sei es nur, um die Studierenden als neue

Käuferschichten zu erschließen.

Einer kritischen Begleitung bedarf auch der Umgang mit den Daten des wissenschaftlichen und nicht-wissenschaftlichen Personals. Fragen des Arbeitnehmerdatenschutzes machen keinen Bogen um die Hochschulen. Von besonderer Brisanz ist die Evaluation von Forschung und Lehre, die immer wieder Fragen aufwirft. Bei allem Verständnis für den Wunsch der Studierenden, sich frei über die Lehrenden auszutauschen, macht es einen gewaltigen Unterschied, ob dies innerhalb der jeweiligen Hochschule oder in der weltweiten Öffentlichkeit des Internet geschieht, in der sich der Betroffene gegen falsche Behauptungen und unfaire Kritik nicht wirksam wehren kann.

Eine besondere Rolle bei dieser Entwicklung spielen Sie, die Datenschutzbeauftragten in den Hochschulen und wissenschaftlichen Einrichtungen. Sie haben den Auftrag, auf die Umsetzung der datenschutzrechtlichen Bestimmungen hinzuwirken. Von Ihrer Fachkenntnis, Ihrem Problembewusstsein und Ihrem Engagement hängt die Gestaltung dieser Entwicklung ab. Das Rad muss aber nicht immer wieder neu erfunden werden. Nutzen Sie daher das Gespräch und den Austausch hier auf dieser ersten Fachtagung mit den anderen Datenschutzbeauftragten von Hochschulen und wissenschaftlichen Einrichtungen und auch mit Vertretern der Datenschutzbehörden! Dann kann diese Tagung zu einem ersten Knoten eines neuen Kompetenznetzes werden.

Donnerstag/Freitag, 9./10. Oktober 2008

2. Fachtagung für Datenschutzbeauftragte an Hochschulen und anderen wissenschaftlichen Einrichtungen

Freie Universität Berlin

weitere Informationen unter www.datenschutz.fu-berlin.de



Datenschützer fordern stärkeres Rechtsbewusstsein der Hochschulen

Pressemitteilung der Datenschutzbeauftragten Niedersächsischer Hochschulen vom 21.02.2008

Datenschutzbeauftragte niedersächsischer Hochschulen beanstanden die ständigen Verstöße gegen das Grundrecht auf informationelle Selbstbestimmung bei der Verarbeitung personenbezogener Daten in ihren Hochschulen. So halten beispielsweise bei der Beurteilung von Lehrveranstaltungen viele Hochschulen die durch das Niedersächsische Hochschulgesetz geforderte Verpflichtung zur Erstellung einer Ordnung zur Verarbeitung personenbezogener Daten nicht ein. Vor der Einführung komplexer Systeme zur Datenverarbeitung wird vor der Aufnahme dieser Verarbeitung keine Risikoabschätzung der möglichen Gefahren für die Betroffenen vorgenommen. Nicht mehr benötigte Daten werden nicht gelöscht, sondern bleiben rechtswidrig gespeichert. Mit diesem Verhalten missachten Hochschulen das Grundrecht der informationellen Selbstbestimmung. Dies ist kein Kavaliersdelikt, sondern verstößt eindeutig gegen geltende Gesetze und untergräbt ein die Demokratie sicherndes Grundrecht. Um die Einhaltung dieses Grundrechts zu gewährleisten, fordern die Hochschuldatenschützer das zuständige Fachministerium auf, zukünftig die Wahrnehmung der Aufsichtspflicht auf die Einhaltung des Datenschutzes der von ihm erlassenen Gesetze auszuweiten.

Prof. Dr. Michael Wettern
Sprecher der Arbeitsgemeinschaft Datenschutzbeauftragte Niedersächsischer Hochschulen
Technische Universität Braunschweig, Spielmannstr. 7, 38106 Braunschweig

Dr. Heiner Bielefeldt

„Ich habe nichts zu verbergen" – ein gedankenloser Spruch

„Wer nichts zu verbergen hat, der hat auch nichts zu fürchten" – so lautet das Mantra derjenigen, die aus kontrollpolitischen Interessen für immer weiter reichende Eingriffe des Staates in die informationelle Selbstbestimmung der Menschen plädieren. Der Slogan verfängt. Mit der Bekundung „ich habe nichts zu verbergen" werden Vorschläge für neue sicherheitspolitische Maßnahmen und damit verbundene Freiheitsbeschränkungen oft achselzuckend hingenommen. Der vorliegende Text erhebt Einspruch gegen diese Formel und die sich darin ausdrückende unpolitische Haltung.

I. Sich „bedeckt halten"



Was ist von der Bekundung „ich habe nichts zu verbergen" zu halten? Kann man einem solchen Bekenntnis überhaupt Glauben schenken? Die spontane Reaktion mag Skepsis sein. Denn dass ein Mensch gar nichts zu verbergen hat, entspricht keineswegs der allgemeinen Lebenserfahrung. Vielmehr kann man vermuten, dass es in jeder Biographie Verletzlichkeiten, sensible Punkte gibt, die der oder die Betroffene nicht in der Öffentlichkeit ausgebreitet sehen möchte. Schon deshalb gibt es Grund, den Slogan „wer nichts zu verbergen hat, hat auch nichts zu fürchten" zurückzuweisen.

Wichtiger – und weniger trivial – ist die Überlegung, dass man sich nicht wirklich *wünschen* kann, dass die Bekundung „ich habe nichts zu verbergen" zutrifft. Man kann eigentlich nur *hoffen*, dass sie nicht stimmt. Denn ein Leben, in dem es nichts zu verbergen gäbe, wäre ein Leben ohne Intimität, ohne Privatheit, ohne Schamgrenzen, ohne persönliche Geheimnisse und ohne Überraschungen – kurz: eine eher armselige Existenz. Sarkastisch formuliert: Wer wirklich nichts zu verbergen hätte, hätte tatsächlich nicht mehr viel zu verlieren.

Wer nichts zu verbergen hätte, könnte im Übrigen auch nichts Substanzielles mitteilen. Ohne die Option, sich gelegentlich „bedeckt" zu halten, d.h. Informationen nicht sofort, zu jeder Zeit preiszugeben, würde menschliche Kommunikation zu Belanglosigkeiten verflachen. Bekanntlich gibt es einen Typus von Mitteilungen, bei denen es uns gleichgültig ist, wer zuhört. Handy-Durchsagen über Zugverspätungen wären ein Beispiel dafür. Sie können zu jeder Zeit und an jedem Ort und auch in Gegenwart beliebiger Dritter geschehen (sofern man in Kauf nimmt, dass diese sich womöglich über die Ruhestörung ärgern).

Wer hingegen Wichtiges mitzuteilen hat – zum Beispiel Schuld oder Versagen eingestehen muss, Sympathie bekunden will oder ein „ernstes Wort" mit jemandem zu reden hat –, muss den dafür *passenden Moment* abwarten. Bis der richtige Zeitpunkt gekommen ist, wird er Zurückhaltung üben und sich „bedeckt" halten müssen. Die Fähigkeit zu persönlicher Zurückhaltung ist nach Helmuth Plessner die Voraussetzung wesentlicher Mitteilung: „Wir bedürfen der Hemmung um unserer selbst willen, der Verhaltung, der Stauung, um Gefälle zu haben."[1]

Neben dem passenden Zeitpunkt braucht substanzielle personale Kommunikation außerdem den *richtigen Ort*. Nicht alles lässt sich überall sagen. Ein Gespräch unter vier Augen in geschütztem Raum ist etwas Anderes als der Smalltalk am Stehtisch beim Sektempfang. Menschen können in der Gynäkologie anders sprechen als im Friseursalon; sie können im Anwaltsbüro oder im Beichtstuhl Informationen preisgeben, die sie nicht unbedingt in der Betriebskantine ausplaudern würden; und sie können im privaten Wohnzimmer intensiver aufeinander eingehen als im allgemein zugänglichen Fahrstuhl. Diese Differenz kommunikativer Räume zu missachten, gilt – einer sich schon seit Längerem ausbreitenden Tendenz zum sozialen und medialen Exhibitionismus zum Trotz – immer noch als Taktlosigkeit.

Deshalb ist es wichtig, dass die unterschiedlichen Räume menschlicher Kommunikation gegeneinander *abgrenzbar* sind und dass diese Abgrenzung auch *verlässlich* bleibt. Die konkreten Grenzlinien zwischen unterschiedlichen Räumen – zwischen geschützter Privatheit und gesellschaftlicher Öffentlichkeit oder auch die Abgrenzung besonders geschützter Räume wie einer Arztpraxis, eines Anwaltsbüros oder des Beichtstuhls – mögen historisch variabel sein (was nicht heißt, dass sie gleichgültig sind!). Entscheidend ist vor allem aber, dass solche Grenzlinien überhaupt existieren, und dass sie klar *erkennbar* und *verlässlich* sind.

Der Verlust verlässlicher Abgrenzung zwischen unterschiedlichen Räumen menschlicher Kommunikation würde nicht nur die private Kommunikation beeinträchtigen, sondern sich letztlich auf das *gesamte Kommunikationsverhalten* der Menschen auswirken. Er hätte Folgen für die *Gesellschaft im Ganzen*, d.h. für alle gesellschaftlichen Bereiche und nicht zuletzt auch für die Politik. Bereits vor über fünfzig Jahren hat Hannah Arendt darauf hingewiesen, dass die Erosion der Privatheit auch die öffentliche Sphäre politischen Redens und Handelns betrifft, weil öffentliches In-Erscheinung-Treten den Gegenhalt einer integren Privatsphäre braucht: „Wir alle kennen die eigentümliche Verflachung, die ein nur in der Öffentlichkeit verbrachtes Leben un-

1 Helmuth Plessner, Grenzen der Gemeinschaft. Eine Kritik des sozialen Radikalismus (1924), in: Gesammelte Schriften, Frankfurt a.M. 1980ff, Bd. V, S. 7-133, hier S. 91.

vermeidlich mit sich führt. Gerade weil es sich ständig in der Sichtbarkeit hält, verliert es die Fähigkeit, aus einem dunkleren Untergrund in die Helle der Welt aufzusteigen; es büßt die Dunkelheit und Verborgenheit ein, die dem Leben in einem sehr realen, nicht-subjektiven Sinn seine jeweils verschiedene Tiefe geben.“[2] Für Arendt ist die Integrität der Privatsphäre deshalb ein eminent „republikanisches“ Anliegen.

II. Freiheit als Definitionsmerkmal des Rechtsstaats

Informationelle Selbstbestimmung ist ein Bestandteil persönlicher und kommunikativer Freiheit. Der Respekt der Freiheit wiederum ist nicht nur ein – vielleicht wichtiges – Rechtsgut neben anderen Rechtsgütern, sondern zugleich Definitionsmerkmal der Rechtsstaatlichkeit. Denn die gebotene Achtung der Würde des Menschen als eines Subjekts freier Selbstbestimmung hat für das Selbstverständnis des Rechtsstaats den *Stellenwert einer unhintergehbaren Prämisse*. Was den freiheitlichen Rechtsstaat von anderen Staatsformen unterscheidet, ist die unverbrüchliche Bindung an die Rechtssubjektivität des Menschen, die der Staat als vorgegeben zu respektieren hat. Sie manifestiert sich inhaltlich in der staatlichen Gewährleistung der unver-äußerlichen Menschenrechte, die ihrem Anspruch nach sämtliche gehören.[3]



Die grundlegenden Freiheitsrechte haben deshalb einen herausgehobenen rechtsnormativen Status, der sie der Verrechnung mit sonstigen Interessen – auch mit staatlichen Sicherheitsinteressen – weitgehend entzieht bzw. etwaige Abwägungen mit konkurrierenden Rechtsgütern zumindest unter strenge Bedingungen stellt. Freiheit ist im Rechtsstaat nicht die irgendwann einmal fällige Dividende erfolgreicher Sicherheitspolitik, sondern der hier und jetzt geltende Maßstab staatlicher Legitimität, dessen Beachtung außerdem einer wirksamen Kontrolle unterworfen ist.

Deshalb steht auch die Sicherheitspolitik in einem Rechtsstaat im Dienst der Freiheit. Dies schließt bekanntlich nicht aus, dass es gleichwohl zu Konflikten zwischen konkreten sicherheitspolitischen Maßnahmen und konkreten Freiheitsrechten kommt. Im Falle solcher Konflikte reicht die übliche Berufung auf eine vage „Balance“ zwischen Sicherheit und Freiheit nicht aus.

Schon das rechtsstaatliche Verhältnismäßigkeitsprinzip geht über das Postulat einer bloßen „Balance“ hinaus, indem es im möglichen Konflikt zwischen Freiheit und Sicherheit *die Argumentationslasten zugunsten der Freiheitsrechte* verteilt. Es verlangt, dass etwaige Einschränkungen bzw. Eingriffe einem wichtigen und legitimen Zweck dienen sowie für die Erreichung dieses Zwecks geeignet und erforderlich sind. Das Kriterium der „Geeignetheit“ soll bloß symbolische Maßnahmen, die womöglich lediglich dazu dienen mögen, politische Entschlossenheit zu demonstrieren, ausschließen; und das Kriterium der „Erforderlichkeit“ verlangt die beständige Suche nach dem jeweils mildesten Eingriff zur Erreichung eines sicherheitspolitischen Ziels. Das Verhältnismäßigkeitsprinzip hat somit die kritische Funktion eines Freiheitsverträglichkeitsprüfungsprinzips. Es geht nicht etwa darum, eine „Mitte“ zwischen zwei gleichrangigen Zielen zu definieren (wie dies die Metaphorik des Ausbalancierens suggeriert), sondern die für das Selbstverständnis des freiheitlichen Rechtsstaats konstitutive *Orientierung am Respekt der Rechtssubjektivität des Menschen* im Rahmen des jeweils Möglichen maximal zur Geltung zu bringen.[4]

Außerdem kennt der Rechtsstaat bekanntlich weitere materiale und prozessuale Garantien, die dazu dienen, den Wesensgehalt der Menschenrechte zu schützen und Abhilfe im Falle von Verletzungen zu schaffen. Schließlich gibt es „absolut“ garantierte menschenrechtliche Kernbereiche, die deutlich machen, dass um der Menschenwürde willen Grenzen möglicher Abwägbarkeit zu beachten sind. In seinem Urteil zum sog. Großen Lauschangriff hat das Bundesverfassungsgericht daran erinnert und klargestellt: „Die Privatwohnung als ‚letztes Refugium' ist Mittel zur Wahrung der Menschenwürde. Dies verlangt zwar nicht einen absoluten Schutz der Räume der Privatwohnung, wohl aber absoluten Schutz des Verhaltens

Zypries zur informationellen Selbstbestimmung

Bei einer Sendung des Deutschlandfunks (DLF) offenbarte Bundes-justizministerin Brigitte Zypries, was sie ohne juristische Beratung von einem sensiblen Grundrecht hält: DLF: „Gehört die informationelle Selbstbestimmung nicht mehr zum Verständnis einer modernen Demokratie?“

Zypries: „Doch natürlich. Aber das Recht auf informationelle Selbstbe-stimmung heißt ja nur, dass Bürger darüber informiert werden müssen, wer was von ihnen speichert. Und das hat sich auch als Abwehrrecht gegen den Staat positioniert“ (http://www.dradio.de/dlf/sendungen/hintergrundpoitik/693750/).

2 Hannah Arendt, Vita activa oder Vom tätigen Leben (Englisches Original 1956) 5. Aufl. München 1987, S, 68.

3 Dieser fundamentale Stellenwert freier Selbstbestimmung für das Verständnis der Menschenrechte zeigt sich paradigmatisch in der Präambel der Allgemeinen Erklärung der Menschenrechte von 1948. Sie enthält ein Zitat jener berühmten „vier Freiheiten“, die der amerikanische Präsident Roosevelt im Januar 1941 proklamiert hatte und die später in die „Atlantik-Charta“ der Alliierten aufgenommen wurden: „Rede- und Glaubensfreiheit und Freiheit von Furcht und Not“. Diese vier Freiheiten lassen sich als eine grobe Typologie der verschiedenen einander ergänzenden Arten von Menschenrechten lesen. Während die Redefreiheit für die politischen Freiheitsrechte (z.B. Meinungsfreiheit, Versammlungsfreiheit und das demokratische Wahlrecht) steht, repräsentiert die Glaubensfreiheit die geistigen Freiheitsrechte, die der Achtung vor den tragenden Gewissens- und Glaubensüberzeugungen des Menschen geschuldet sind. Die Freiheit von Furcht lässt sich mit den Justizgrundrechten in Verbindung bringen, die Schutz vor willkürlicher Inhaftierung und Fairness im Gerichtsverfahren garantieren. Mit der Freiheit von Not verweist die Präambel schließlich auf die wirtschaftlichen und sozialen Rechte, die ebenfalls Freiheitsansprüche darstellen.

4 Vgl. Heiner Bielefeldt, Freiheit und Sicherheit im demokratischen Rechtsstaat. Essay hg. vom Deutschen Institut für Menschenrechte, Berlin 2004.

in diesen Räumen, soweit es sich als individuelle Entfaltung im Kernbereich privater Lebensgestaltung darstellt."[5]

III. Rechtsstaatlichkeit als Solidaritätsstruktur

Es gibt Anzeichen dafür, dass der Stellenwert informationeller Selbstbestimmung in der öffentlichen Debatte in jüngster Zeit wieder zugenommen hat. Weit reichende sicherheitspolitische Vorschläge – bis hin zur Forderung nach Einführung kriegsrechtlicher Kategorien in die Innenpolitik[6] – haben dazu beigetragen, dass gleichzeitig auch eine neue Sensibilität für die Kultur der Rechtsstaatlichkeit zu entstehen scheint.

Das Unbehagen angesichts einer immer engmaschigeren gesellschaftlichen und staatlichen Kontrolle des Einzelnen artikuliert sich typischerweise als Angst vor dem „Generalverdacht". Ein jeder, so die vorgetragene Sorge, könne ohne eigenes Zutun in die Maschinerie sicherheitspolitischer Kontrollmaßnahmen geraten und dabei ggf. erhebliche berufliche, soziale und persönliche Nachteile erleiden.



Der Topos vom drohenden Generalverdacht appelliert an das aufgeklärte Selbstinteresse jedes Einzelnen. Was dabei zu kurz kommt, ist die Einsicht, dass Rechtsstaatlichkeit zugleich eine *solidarische Struktur* hat. Die Freiheitsrechte, die jedem einzelnen zugute kommen, haben aller Erfahrung nach *besondere Bedeutung* für solche Menschen, die sich in Lebensweise, kultureller Prägung, Hautfarbe, sozialer Lage, gesellschaftlichem Status, politischer Einstellung oder anderen Merkmalen vom gesellschaftlichen Mainstream deutlich unterscheiden. Zwar sind die elementaren Freiheitsrechte – als Menschenrechte – mit dem Menschsein jedes Menschen verbunden und stehen daher jedem Menschen gleichermaßen zu. Gleichwohl gilt, dass sie für die Entfaltungsoptionen von Minderheiten, gesellschaftlichen Dissidenten, „Quertreibern" und solchen Menschen, die „irgendwie anders" zu sein scheinen, erfahrungsgemäß eine *erhöhte Relevanz* entfalten. Solche Menschen sind es denn auch, die von einer Rückentwicklung der Rechtsstaatlichkeit aller Voraussicht nach besonders betroffen sein dürften.

Der Topos vom drohenden Generalverdacht überdeckt, dass die mit etwaigen Erosionserscheinungen der Rechtsstaatlichkeit verbundenen Risiken keineswegs gleichmäßig auf die Gesamtbevölkerung verteilt sind. Es gibt Menschen, die aufgrund ihres Aussehens, ihrer Herkunft, ihrer Lebensweise, ihrer politischen Einstellung oder Artikulationsfähigkeit, ihrer sexuellen Orientierung oder sonstiger Merkmale mutmaßlich stärker betroffen sein dürften als andere. Mit anderen Worten: Neben der Gefahr des Generalverdachts, von der oft die Rede ist, bestehen auch Gefahren eines *pauschalen Spezialverdachts*, der dazu führt, dass bestimmte Bevölkerungsgruppen – nennen wir sie „Menschen in besonders verletzlichen Lebenslagen" – die Folgen eines Rückbaus rechtsstaatlicher Freiheitsgewährleistungen aller Voraus-sicht nach überproportional zu spüren bekommen würden.

Der Rechtsstaat dient nicht nur dem Freiheitsinteresse des jeweils Einzelnen, sondern er repräsentiert darüber hinaus auch die *Bereitschaft der Gesellschaft*, für die Freiheitsinteressen der Mitmenschen – insbesondere auch von besonders bedrohten gesellschaftlichen Minderheiten bzw. von Menschen in besonders verletzlichen Lebenslagen – gemeinsam einzustehen. Was für den *Sozialstaat* gilt – nämlich dass darin die überproportionalen Lebensrisiken von Menschen in besonders verletzbaren Situationen solidarisch von der Gemeinschaft mit getragen werden – gilt mutatis mutandis eben auch für den *Rechtsstaat*. Während diese solidarische Komponente in der öffentlichen Diskussion über die Weiterentwicklung des *Sozialstaats* mehr oder minder selbstverständlich vorausgesetzt zu werden scheint, kommt sie in der Debatte über den *Rechtsstaat* merkwürdiger-weise kaum je zu Wort.

Dem lapidaren Motto „ich habe nichts zu verbergen" die Gefahren eines sich ausbreitenden Generalverdachts entgegenzuhalten reicht nicht aus. Es muss deutlich werden, dass Rechtstaatlichkeit nicht nur im aufgeklärten Selbstinteresse des Einzelnen begründet ist, sondern die Bereitschaft zum republikanischen und solidarischen Engagement für die Freiheitsrechte aller – insbesondere der Menschen in verletzlichen Lebenslagen – verlangt. Der Spruch „ich habe nichts zu verbergen" ist eben auch deshalb so ärgerlich, weil er eine unpolitische Verengung der Perspektive auf die erste Person Singular ausdrückt. Die angemessene Frage ist demgegenüber gerade nicht, *ob ich* etwas zu verbergen habe, sondern *ob wir* uns zu einer Gesellschaft entwickeln wollen, in der von vornherein nur derjenige einigermaßen unbehelligt leben kann, der sich damit abfindet, dass er nichts mehr verbergen kann. Dass die Antwort auf diese Frage nur ein klares Nein sein kann, wird hoffentlich breite Zustimmung finden.

5 Urteil des Bundesverfassungsgerichts zum sog. Großen Lauschangriff vom 3. März 2004, Rdnr. 120f.

6 Vgl. z.B. Otto Depenheuer, Selbstbehauptung des Rechtsstaats, Paderborn 2007.

BVerfG-Vizepräsident Hassemer fürchtet um Datenschutz

Gemäß dem Vizepräsidenten des Bundesverfassungsgerichts (BVerfG) Winfried Hassemer wird der Datenschutz in Deutschland immer weiter aufgeweicht: „Meine Sicht ist, dass man sich den Staat nicht mehr durch anständiges Verhalten vom Halse halten kann. Wir überschauen nicht mehr, in welche Dateien wir aufgenommen werden." Das kollidiere mit der verfassungsrechtlichen Anforderungen, dass man als Bürger wissen sollte, wo welche Daten gespeichert sind. „Wir haben ohne Anlass eine Überwachung des Bürgers, die weit geht". Der beste Schutz dagegen sei, keine „Datenspuren" zu legen. So benutze er keine Kundenkarten. Hassemer warnte das Parlament vor einer Arbeitsteilung nach dem Muster: Die Politik wird in Berlin gemacht, die Grundrechte werden in Karlsruhe überwacht: „Auch Bundestagsabgeordnete wenden das Grundgesetz an"
(SZ 22./23.12.2007, S. 6).

Martin Rost

Datenschutz und Datensicherheit an deutschen Hochschulen

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hatte 2007 erneut einen Anlauf genommen und sich mittels zahlreicher Beratungsgespräche, einer umfänglichen Prüfung vor Ort und eines Audits einen umgreifenden und tiefen Einblick in die Situation des Datenschutzes bei den landeseigenen Hochschulen verschafft. Das am Ende des Jahres zu ziehende Fazit überraschte wenig: Es ist nach wie vor auffallend schlecht um den Datenschutz an den Hochschulen bestellt. Besonders alarmierend ist, dass sich überwiegend auch keine Bestrebungen oder Strategien abzeichnen, diesen Zustand zu verändern. Schon aus Gründen der Verbesserung ihrer Governance müssen Strategen und Verantwortliche an den Hochschulen alles unternehmen, um endlich Transparenz in ihre EDV-gestützten Verfahren, Workflows und Geschäftsprozesse zu bekommen.



Hochschulen können durchgängig keine hinreichend belegte Auskunft darüber geben, welche personenbezogenen Daten ihrer Klientel, Studierenden und Mitarbeiter sie auf welche Weise und von wem verantwortet verarbeiten oder zugänglich machen. Nirgends gibt es den Ansatz eines gezielt entwickelten, nachhaltigen Datenschutz-managements, wie er in anderen Organisationen länger schon, in Abstimmung mit der Innenrevision, dem Finanzcontrolling oder dem Sicherheitsbeauftragten der EDV, zumindest auf den Weg gebracht wurde. Die Datenschutzbeauftragten vor Ort kennen den Modus des akuten Reparierens – und halten diesen Modus, zusammen mit der Hochschulleitung, eigentlich auch für den ganz normal nur einnehmbaren. Manchmal sind die Datenschutzbeauftragten der Hochschulen sogar unsicher über ihren eigentlich Arbeitsgegenstand, wenn sie sich bspw. primär aufgerufen fühlen, die Welt über die Gefahren der modernen Technik für den Datenschutz aufzuklären, anstatt ihre eigene Organisation im Hinblick auf Datenschutz-verstöße zu beobachten.

In den Gesprächen anlässlich der ersten Konferenz für Datenschutzbeauftragte an den Hochschulen, die im September 2007 an der Freien Universität Berlin stattfand, zeigte sich, dass diese Verallgemeinerungen dieser schleswig-holsteinischen Befunde erlaubt sind. Und ein Blick in die Tätigkeitsberichte der Landesdatenschutzbeauftragten allein der letzten vier Jahre bestätigt die nachfolgend aufgelisteten Einzelbefunde. Die Datenschutz-situation an deutschen Hochschulen ist von je her bestürzend schlecht.

Man trifft an den Hochschulen zwar allseits ein im persönlichen Gespräch durchaus glaubwürdiges Bekunden von Sensibilität für Datensicherheit und Datenschutz sowohl bei den Hochschulleitungen als auch den für die Technik Verantwortlichen an. Doch sobald man die übergreifenden Prozesse, die verarbeiteten Daten und die Rollenzuschnitte und Zugriffsregelungen vor Ort einmal ganz konkret im Detail in den Blick nimmt und diese dann mit den gesetzlichen Regelungen abgleicht, erzielt man schnell Einigkeit darüber, dass es um die Datenschutzwirklichkeit sehr schlecht bestellt ist. In der Verwaltung der Hochschulen ist in der Regel professionell ausgebildetes, Rechtskonformität anstrebendes Verwaltungs-know-how anzutreffen, in der Systemadministration überwiegen Kompetenz und Orientierung am aktuellen Stand der Technik. An den zumindest teil-autonom agierenden Instituten wird dagegen, von einigen wenigen Ausnahmen abgesehen, hemdsärmelig, nachlässig und frei von rechtlichen oder fortgeschrittenen sicherheitstechnischen Kenntnissen in Bezug auf die rechtlichen und technischen Datenschutzanforderungen agiert.

Da wurden beispielsweise, um einen konkret gemeldeten typischen Vorfall zu nennen, Dateiserver, die für die private Heimnutzung billig konzipiert über keine Sicherheits- oder differenzierte Authentisierungsmechanismen verfügen, mal eben zu bereits be-stehenden zentralen Fileservern hinzugefügt. Auf diesem Dateiserver lagen fortan monatelang Dateien mit Forschungsprojektanträgen herum, die sensible personenbezogene Daten enthielten. Die Motive für derartiges Ad-hoc-Handeln in Bezug auf EDV gleichen sich inzwischen seit Jahrzehnten: Notorisch wenig Geld und zu wenig Plattenplatz.

Ebenso typisch wie der ungeregelte Umgang mit Plattenplatz ist der in den rechtlich wesentlichen Aspekten ungeregelte Umgang mit E-Mail-Accounts. So wird die private Nutzung von E-Mail-Accounts an den Unis relativ umstandslos erlaubt. Zugleich lässt sich die Uni in den immerhin durchgängig vorhandenen Benutzerordnungen das Zugriffsrecht auf derartig private Daten ebenso umstandslos einräumen. Wenn dann Polizei oder Staatsanwaltschaft die Herausgabe von Daten über Studierende einfordern, wird den Forderungen schlicht entsprochen, obwohl das Briefgeheimnis hochrangig im Artikel 10 des Grundgesetzes formuliert ist. Mit dem Ausscheiden von Personen werden E-Mail-Accounts ebenso gern platt gelöscht wie jahrelang stehen gelassen. Und es gibt dann niemanden, dem die auf diese Weise entstehenden Datengräber auf den Systemen auffallen, zumindest solange nicht, bis ein Administrator, rechtlich möglicherweise grenzwertig durch das System vagabundierend, hin und wieder aufgrund zufälliger Kenntnisse über solche Accounts stolpert. Und dann? Wer ist für die Löschung verantwortlich? Es gilt festzulegen und an die Betroffenen zu kommunizieren, wie die Maßnahmen für die rechtlichen, organisatorischen und echnischen Anforderungen insgesamt im Lebenszyklus eines E-Mail-Accounts an einer Hochschule umgesetzt sind.

Ein weiteres Beispiel für das Problem, methodisch geregelte Prozesse in den Hochschulen einzuführen, betrifft die Abbildung von Prüfungsordnungen in der EDV. So wurde eine veränderte Prüfungsordnung in der Software zur Studierendenverwaltung durch einen (eigentlich von Projektgeldern finanzierten) Hilfswissenschaftler auf bloßen Zuruf durch Umkonfiguration umgesetzt. Nach der Konfiguration wurde das Programm, vielleicht und irgendwie, aber in keinem Fall prüfbar dokumentiert, getestet. Der Sinn eines Test-und-Freigabe-Prozesses besteht darin, dass die Verantwortung für eine fachgerechte technische Implementation und Konfiguration eines Regelwerks, das große Bedeutung für die davon Betroffenen hat, als erbracht gelten kann und anschließend die Verantwortung für den korrekten Ablauf vom Fachverantwortlichen übernommen wird.

Eine Sekretärin eines Instituts demonstrierte anlässlich einer Prüfung, wie trivial es für sie möglich ist, die Noten Studierender einzusehen, und zwar auch die anderer Fakultäten, zu denen sie überhaupt keinen Bezug hat. Und weil sie sogar die Passworte einsehen konnte, mit denen die Professoren sich über das Internet von ihren heimischen PCs auf die universitätsinternen Server einloggen können, um Daten ihrer Studentinnen und Studenten zu bearbeiten, hätte sie diese Noten, durch keinen Mechanismus kontrollier- und korrigierbar, verändern können. Dies wurde dann sofort abgestellt. Aber allein der Umstand, dass es durchaus problematisch ist, wenn Professoren von ihren zumeist dilletantisch administrierten heimischen PCs aus – und warum dann nicht auch hin und wieder mal aus einem zwielichtigen Internet-Cafe heraus? – derartige Arbeiten verrichten können, traf bei Beteiligten vor Ort wieder auf Unverständnis. Zwar war in diesem konkreten Fall die Verbindung per https SSL-verschlüsselt, doch liegt darunter kein tatsächlich kontrolliertes Zertifikate-Handling, wie es heutzutage etwa beim Online-Banking eine Selbstverständlichkeit ist. Mag man auch Sekretärin vom Zugriff aussperren können, bei Systemadministratoren geht das grundsätzlich nicht. Systemadministratoren sind auf einem System allgewaltig und können sozusagen von „hinten“ grundsätzlich an alle Daten herankommen – und nicht nur an die persönlichen Daten der Mitarbeiter und Studierenden, sondern bspw. auch an die Rohdaten von Forschungsprojekten oder an Examens- und Doktorarbeiten. Dass das so ist, muss allgemein bekannt sein. Und es müssen organisatorische Vorkehrungen getroffen werden, damit ein Systemadministrator, wenn er mit Superuser- bzw. Root-Rechten auf dem System arbeitet, dies nicht unbeobachtet macht. Die Strategie muss sein, dass jegliche Handlung in einer Organisation transparent ist und u.a. auf ihre Rechtmäßigkeit hin überprüft werden kann. Systemadministration muss nicht vertrauensselig hingenommen werden. Hier kann insbesondere der betriebliche Datenschützer für entsprechende organisatorische Schutzvorkehrungen sorgen.



Ein wesentlicher Aspekt von Datenschutz in Organisationen besteht generell darin, für alle Beteiligte – für die Mitarbeiterinnen und Mitarbeiter ebenso wie für das organisationsexterne Klientel – Transparenz in die mehr oder weniger organisierten Prozesse zu bringen. Transparenz ist die Voraussetzung dafür, dass Prozesse intern geregelt, geplant und gesteuert werden können, dass Verantwortung für die Prozesse übernommen werden kann, dass die Wirtschaftlichkeit und Gesetzeskonformität von Prozessen und Entscheidungen nachweisbar wird und dass extern die Betroffenen gegebenenfalls der Verarbeitung ihrer personenbezogenen Daten widersprechen können. Deshalb müssen gemäß den Landesdatenschutzgesetzen die Prozesse von Organisationen dokumentiert werden. Erfahrungsgemäß lernen Organisationen mit der Anforderung zur Dokumentation ihre Prozesse überhaupt erst in einem hinreichenden Auflösungsniveau kennen.[1] Wir stellten an sämtlichen Hochschulen fest, dass kein einziger IT-gestützter Kernprozess etwa in der Verwaltung hinreichend dokumentiert war. Einzig Dokumente, die die Nutzungsbedingungen der EDV für Studierende betrafen, waren allseits in eine einigermaßen akzeptable Form gebracht. Doch schon bei Dienstanweisungen für die Sachbearbeiter der Hochschulverwaltung hörte es wieder auf, es lagen schlicht keine vor. Es konnten keine aktuellen Organigramme der Hochschulorganisation vorgelegt werden, ebensowenig gültige Geschäfts-verteilungspläne oder Tätigkeits-beschreibungen insbesondere für die allmächtigen Systemadminis-tratoren. In einem einzigen Fall konnte man zwar so etwas wie eine angefangene Inventarliste von Hardware und Software zumindest für einen klar abgegrenzten Bereich vorlegen. Es fehlten durchgängig Dokumente für IT- und Verfahren oder Sicherheitsmaßnahmen, die einen definierten Sicherheitsbedarf operativ erfüllen. Über die Aktivitäten, die dabei automatisiert zu protokollieren und zu prüfen sind, war man sich vollkommen im Unklaren, entsprechend gab es keine geregelten Verfahren zum Umgang mit den massenhaft anfallenden Protokolldaten, insbesondere denen über die Tätigkeiten der Systemadministration. Zwar konnten in allen Fällen Netzwerkpläne vorgelegt werden, ohne die eine Administration in einem Computernetz sowieso undenkbar ist. Nur waren diese dann weder aktuell noch methodisch zureichend gestaltet. Zum Teil waren Testsysteme für Software, die in „Produktion“ war, vorhanden. Aber es konnte wiederum keine Dokumentation erfolgter Tests und deren Ergebnisse sowie keine Freigaben der Software für die Produktion durch die Fachverantwortlichen vorgelegt werden. Letzteres ist ein Indikator dafür, dass der rechtlich bedeutsame Akt der Übergabe der Verantwortung vom installierenden, konfigurierenden und Funktionen testenden Computerspezialisten auf den inhaltlich testenden Fachverantwortlichen ungeregelt ist. Tatsächlich war man vereinzelt noch der Ansicht, dass grundsätzlich nicht der Fachverfahrensverantwortli che sondern die Technikabteilung die Verantwortung für die EDV-gestützten Verfahren habe. Derartig die Rechtslage verkennende Statements

1 Man misst den Reifegrad von Prozessen mittels eines 5-stufigen Maturity-Modells: Von Stufe 1 „man hat einen Input und man hat einen Output“ bis zur Stufe 5 mit dokumentierten Prozessen, die man je nach funktionaler Anforderungen neu zusammensetzen kann.

hört man in Privatunternehmen oder öffentlichen Verwaltungen lange nicht mehr. Die Einrichtung der Zugriffsrechte der Hochschulleitung oder des Verwaltungspersonals oder des akademischen Lehrapparats auf Dateiserver oder personenbezogene Daten von Studierenden konnte in keinem Falle dokumentiert werden. Ebenso wenig konnte man dokumentieren, ob die Hochschulleitung, Dekane oder Systemadministratoren, etwa im Rahmen von Revisionsverfahren oder aufgrund von Sicherheitsvorfällen, in der Vergangenheit außergewöhnliche Zugriffe auf personenbezogene Daten genommen haben. Es gab keine Dokumentation darüber, ob es Sicherheitsvorfälle gab und wie diese gesteuert wurden. Verträge mit externen Dienstleistern, insbesondere den IT-Dienstleistungen der „Hochschul-Informations-System GmbH" (HIS) oder mit lokalen EDV-Häusern, die bestimmte Vor-Ort-Services leisteten, fehlten entweder völlig oder waren unzureichend. Und nicht zuletzt herrscht durchgängig weitgehend Unkenntnis geltender Rechtsvorschriften insbesondere auf der Ebene von Fakultäts-, Instituts- oder Fachbereichs-Vertreterinnen und Vertreter vor.



Die Datenschutzbeauftragten waren in der Regel mit geringen Zeit-kontingenten ausgestattet (von 5% bis 50% ihrer Arbeitszeit), verfügten durch die Bank über nur geringe technische Kenntnisse und hatten keine auf Nachhaltigkeit zielenden Strategien mit Gestaltungsanspruch eines umfassenden Datenschutzmanagementsystems entwickelt. Ihnen verblieben einzig einige anlassbezogene Aktivitäten. Immerhin konnten in einem Fall einige Artikel vorgelegt werden, in denen in der lokalen Hochschulzeitung auf Datensicherheitsaspekte hingewiesen wurde, sowie Schulungen zur Weiterbildung bei der Daten-schutzakademie. Sie wussten durchgängig von keinem Sicherheits-vorfall zu berichten, sie waren dementsprechend nie an deren Management beteiligt worden. Entsprechend war den Datenschutzbeauftragten der Gedanke fremd, im Rahmen eines Sicherheitsmanagements bei Sicherheitsvorfällen bestimmter Qualität, in denen oftmals an vielen bestehenden Richtlinien vorbei gehandelt wird, die zwangsläufige Beteiligung schlicht einzufordern. Auch muss man vermuten, dass die Bewertung eines Vorfalls als Sicherheitsvorfall so gar nicht vorgenommen wird.

Und das ist das Beunruhigende beim langjährigen Blick auf Hochschulen: Während anderenorts, in öffentlicher Verwaltung und Wirtschaft, die Konzepte etwa zum Risikomanagement à la IT-Infrastructure Library („ITIL") sowie IT-Architekturstrategien wie Service-Oriented-Architectures („SOA") oder die Durchleuchtung der eigenen Sicherheitsmaßnahmen nach BSI-Grundschutz oder der Aufbau eines IT-Sicherheits- und Datenschutzmanagements inzwischen zum langweilig gewordenen Alltag gehören, hat man an den Hochschulen noch nicht einmal angefangen, sich mit diesen Strategien und Konzepten der Verschränkung von Aufgabenstellungen, Organisation und IT-Services überhaupt nur ernsthaft zu beschäftigen. Vor Ort, beim einzelnen Administrator, findet man da durchaus Vorstellungen darüber, welche Vorteile beispielsweise der Betrieb eines zentralen Helpdesks brächte, um mit Hilfe eines Ticketsystems im Backofficebereich das Incident- und Changemanagement der gesamten Hochschule effektiver als bislang zu organisieren. Aber auf Seiten der für die Hochschulorganisation Verantwortlichen scheint es so zu sein, dass diese meinen, mit der stärkeren Verwirtschaftlichung der Hochschultätigkeiten in den vergangenen 15 Jahren alles Wesentliche entschieden zu haben.

Dabei lassen sich Hochschulen nach wie vor kaum steuern. Dieser Bedarf an Intransparenz lässt sich nicht auf die notwendige Freiheit für Forschung und Lehre in den Fakultäten zurückführen und lässt sich auch nicht dadurch nachhaltig austrocknen, indem man unter größten Mühen ein verbessertes Finanz-Controlling implementiert oder die Ausbildung verschult. Im Kern gilt es, die Produktionsseite von Hochschulen zu professionalisieren, also insbesondere den Wahrheit-konstitutiven Aspekt des wissenschaftlichen Diskurses technisch zu unterstützen. Erst wenn dieser Kern der Produktion, Konsumtion und Distribution von Diskursbeiträgen auf dem Niveau industrieller Produktion angelangt ist, greifen auch die modernen Steuerungsinstrumente, wird es zu einer Professionalisierung auch der Hochschulorganisation kommen. Man kann Hochschulen, weil sie organisatorisch und mental bislang nicht in der industrialisierten Moderne angekommen sind, sondern noch immer in zunftähnlichen Strukturen verhaftet sind[2], auch nicht mit den Mitteln der Moderne steuern. Entsprechend schlecht ist es um die reale Datenschutz-Awareness und das Datenschutzmanagement in Bezug auf die Mitarbeiter unter den Wissenschaftlern und der Verwaltung, etwaigen Versuchspersonen und nicht zuletzt der Studenten bestellt. Datenschutz, möglicherweise verstanden sogar im modern-umfassenden Sinne einer ganzheitlichen Kommunikationsökologie, ist an Hochschulen, anders als in anderen Organisationen, bislang kein relevantes Thema.

Was ist zu tun? Einfach nur mehr Ressourcen für den Datenschutzbeauftragten (DSB) einzufordern ist allein wenig zielführend. Ressourcen gibt es nur, wenn die oder der DSB etwas wertschöpfend Funktionales für die Organisation zu bieten hat. Sie oder er sollte deshalb zumindest soviel Professionalität aufweisen, um als ein aktiver Wächter der Rechtmäßigkeit insbesondere im Umgang mit personenbezogenen Daten auftreten zu können. Damit sind nicht nur Kenntnisse der einschlägigen Datenschutzgesetze gemeint, sondern generell Kenntnisse darüber, welche Regelwerke (Gesetze, Verordnungen, Verträge, Leitlinien) gelten und wie geforderte Regelkonformität herstellbar ist. Ein DSB sollte aktiv nach Bündnispartnern mit Interessensschnittmengen suchen, also vor allem mit dem Personalrat bzgl. Mitarbeiter-Datenschutz ins Gespräch kommen, mit Studierendenvertretern sprechen und den Kontakt zum

2 Rost, Martin, 2001: Zur Produktion des Wissens im digitalen Zeitalter; in: Universität Erfurt/ Heinrich Böll-Stiftung 2001: Universitäten in der Wissensgesellschaft (Erfurter Universitätsreden), München, Iudicium-Verlag. http://www.maroki.de/pub/sociology/mr_wkdz.html

Sicherheitsbeauftragten des Rechenzentrums suchen. Mit dem Leiter des Rechenzentrums bzw. dem EDV-Leiter lässt sich eine Dokumentationsstrategie der Verfahren und der Technik vereinbaren. Man sollte damit beginnen, die HIS aufzufordern, zu dokumentieren, was dort wo und in welcher Form protokolliert wird und unter welchen Umständen wer warum und wie diese Daten ausgewertet und wie mit dann möglicherweise festgestellten Sicherheitsvorfällen und Datenschutzverstößen verfahren wird. Und der Hochschulleitung ist darzulegen, dass Datenschutz heutzutage zu einem konstruktiven Aspekt des Qualitäts- bzw. Risk-Managements einer Organisation geworden ist. Datenschutz heute heißt: Konstruktive Beteiligung am Kommunikationsmanagement nach Innen und Außen.

Dr. Kai-Uwe Loser

Zum Stand der Entwicklung von E-Learning-Systemen zwischen informationeller Selbstbestimmung und Freiheit der Lehre

E-Learning im praktischen Einsatz

Die anfänglich euphorischen Hoffnungen in das E-Learning sind inzwischen pragmatischen Anforderungen gewichen. An den Hochschulen ist dennoch ein stetig wachsender Einsatz von Systemen zu bemerken. Es gibt praktisch keine Hochschule in Deutschland mehr, an der nicht mindestens eines der vielen Systeme[1] eingesetzt wird. Die Zeitspanne von der forschenden Entwicklung der Plattformen zum praktischen Einsatz in der Lehre an den Hochschulen ist dabei erstaunlich kurz, was sicherlich auch daran liegt, dass die Rollen von Entwickler und Anwender bei diesen Systemen häufig zusammenfallen. Im Zuge einer solchen außerordentlich schnellen Entwicklung bleibt das Thema Datenschutz jedoch häufig leider auf der Strecke. Wo Forscher sich vor einiger Zeit noch auf die Forschungsfreiheit berufen konnten, ist im heutigen praktischen Einsatz der Systeme immenser Nachholbedarf festzustellen. Der zunächst existierende Forschungshintergrund versuchte die didaktische Wirksamkeit der Unterstützungsmöglichkeit nachzuweisen, zurzeit sind aber viele Systeme zu großen Teilen zur Unterstützung der laufenden Lehre im Betrieb. Dass Forschungseinsatz und Lehrpraxis aus Datenschutzsicht grundlegend verschiedene Anforderungen zu erfüllen haben, ist bei diesem Übergang meist nicht bedacht worden.

1 Eine umfassende aktuelle Übersicht ist schwer, in folgendem Beitrag ist eine Liste von Open-Source Produkten zu finden: von Kiedrowski, Joachim (2004): Open-Source-Software – E-Learning zum Nulltarif? In: Hohenstein, A.; Wilbers, K. (Hrsg.): Handbuch E-Learning. Expertenwissen aus Wissenschaft und Praxis, Seiten 1–15.



E-Learning im praktischen Einsatz

Es gibt auf dem Markt eine ganze Reihe von Produkten, die teils mit hochgradig speziellen Funktionen ausgestattet sind und verschiedene Nischen besetzen. Beispielsweise gibt es spezialisierte Produkte für die Produktion und Verteilung von Videoaufzeichnungen von Vorlesungen. Ein Großteil der Produkte deckt aber Funktionalitäten sogenannter Learning Management Systeme ab. Hier geht es umfassend um die Durchführung von Lehrveranstaltungen. Eine Übersicht über gängige Funktionalität gibt Abbildung 1.

Integration von Web-Funktionalität

Zur Realisierung der Funktionalitäten wurden in der Regel vorhandene Basissysteme mit unterschiedlichem Hintergrund erweitert: Dokumentenmanagement- oder Content-Management-Plattformen bilden typischerweise die Basis. Zudem lassen sich die Entwickler der Systeme gerne von offenen Plattformen aus dem Internet inspirieren. Funktionen wie Diskussionsforen, Wikis oder Selbstdarstellungen sind aus entsprechenden Plattformen entlehnt. Dabei tritt aber ein wesentlicher Aspekt für den Datenschutz zutage: Wo bei Online-Plattformen häufig (zumindest für weitere Nutzer) anonym agiert werden kann und eine symmetrische Beziehung zwischen den verschiedenen Nutzern besteht, sind E-Learningsysteme in ein existierendes soziales System mit einer bereits existierenden Machtstruktur eingebunden. Dadurch sind viele Daten, die in offenen Systemen noch als harmlos einzuschätzen sind, im erzwungenen Hochschulumfeld durchaus problematisch. Ein Beispiel sind die Zeitstempel an Diskussionsbeiträgen, die im Falle von E-Learning Auskunft über die Arbeitsgewohnheiten der Studierenden geben. Einerseits sei dazu angemerkt, dass die Orientierung der Funktionalität an Gewohntem aus dem Netzalltag vieler Studierender durchaus nachvollziehbar ist. Die Nutzer vergleichen die Systeme im Hochschulalltag mit dem, was sie eher im privaten Umfeld nutzen, und erwarten vergleichbare Funktionen: Erwartungskonformität ist





Abbildung 1: Funktionsvielfalt in E-Learning-Systemen



bei der Gestaltung der Systeme also ein durchaus ein beachtenswertes Kriterium. Andererseits zeigt sich in dem geringen Bestreben, auch abweichende Lösungen zu versuchen, eine nur gering ausgeprägte Sensibilität bezüglich Datenschutzfragen.

Analysiert man den praktischen Einsatz von E-Learning-Systemen an Präsenzhochschulen, dann ergibt sich ein Bild bei dem gemäß einer Pareto-ähnlichen Verteilung zunächst über 90% der abgewickelten Veranstaltungen die E-Learning-Plattform vor allem als einfaches „Content-Management-System“ nutzen, um einem eingeschränkten Nutzerkreis von Studierenden leicht Informationen und Materialien zugänglich zu machen. Dabei wird dann nur ein Bruchteil der Funktionalität tatsächlich benötigt. Eines der Ziele in diesem Szenario ist es auch urheberrechtliche Probleme zu vermeiden, indem Materialien eingeschränkten Nutzerkreisen zur Verfügung gestellt werden.[2] Nur wenige Lehrende nutzen hingegen weitergehende Funktionen im Rahmen spezialisierter didaktischer Konzepte. Meist sind das eher seminarähnliche Situationen, in denen kleinere Arbeitsgruppen über die Kooperationsmöglichkeiten von E-Learning-Plattformen bei der gemeinsamen Erarbeitung von Inhalten unterstützt werden. Diese Verteilung in der tatsächlichen Nutzung der Systemfunktionalitäten ist in der Konfigurierbarkeit der Systeme nicht angemessen abgebildet, was für die Protokollierung detaillierter dargelegt wird.

Datenschutz vs. Forschung und Lehre?

Die geringe Sensibilität für den Datenschutz entsteht auch aus dem Übergang der Systeme von der Erforschung der Wirksamkeit der Funktionalität für das didaktische Ziel hin zu einem breiten praktischen Einsatz. Als Forschungsgegenstand lassen sich bestimmte Funktionen begründen und zumindest teilweise müssen diese dann auch als datenschutzrechtlich zulässig angesehen werden. Im breiten praktischen Lehreinsatz sind Funktionen, die das Verhalten der Nutzer detailliert analysierbar machen, aber nicht mehr zu rechtfertigen. Das häufig genannte Argument, dass die Funktionen die Freiheit der Lehre beträfen, ist dabei nicht stichhaltig.[3] Das explizit im Grundgesetz verankerte Recht auf Freiheit in Forschung und Lehre (Artikel 5 GG) bezieht sich auf inhaltliche und methodische Freiheiten. Es ist kein Szenario bekannt, wo tatsächlich die Lehrefreiheit mit der informationellen Selbstbestimmung in Konflikt steht. Die methodischen Entscheidungen sind auch ohne Einschränkungen beim Datenschutz umzusetzen.

Protokollierung im E-Learning

Um die bisher genannten Überlegungen nochmals zu verdeutlichen, soll die Protokollierung als eine gängige Komponente der Systeme detaillierter betrachtet werden. Aus vielen anderen Systemen (Betriebssysteme, Datenbankanwendungen) betrachtet man die Protokollierung eher als ein Anhang des Systems. Protokollierung ist oft nicht unbedingt für die Kernfunktionalität erforderlich, sondern es werden konkrete Nebenziele erreicht (z.B. Revisionssicherheit, Fehlererkennung, etc.). Die zur Absicherung solcher Logfiles existierenden Lösungen[4] sind beim E-Learning aber nicht einsetzbar, da Aufzeichnungen von Nutzerverhalten integraler Bestandteil vieler Funktionen sind. Dass dabei technisch gesehen unterschiedliche Realisierungen gewählt werden, ist für den Sachverhalt aus Datenschutzsicht nicht wesentlich.

Aufgezeichnetes Nutzerverhalten wird also für verschiedene Funktionen genutzt. Die wichtigsten sind dabei:

2 Das Thema Urheberrecht hat dabei bisher weit mehr Beachtung gefunden als der Datenschutz: Kreutzer, Till (2007): Rechtsfragen bei E-Learning - Ein Praxis-Leitfaden. Multimedia-Kontor Hamburg. http://www.mmkh.de/.

3 Vgl. Zilkens, Martin; Heinrich, Christoph (2006): Entbindet die Freiheit von Forschung und Lehre den Hochschullehrer von der Beachtung des Datenschutzes. Recht der Datenverarbeitung 23 (2007), 1, S. 9 – 14.

4 Siehe z.B. Martin Meints (2006): Protokollierung bei Identitätsmanagementsystemen, Anforderungen und Lösungsansätze. DuD 30 (2006) 5; Christian Schmitz (2003): Flight Recording Box – Next Generation Logging: Syslog-NG, Linux-Magazine, 12/2003.

- Aktive Benachrichtigungen: z.B. tägliche E-Mail-benachrichtigungen über Aktivitäten im System (Neueinstellen eines Übungsblattes, Korrektur von Vorlesungsfolien oder ein neuer Beitrag im Diskussionsforum.)
- Anzeigen im System: vor allem zur Hervorhebung von ungelesenen oder noch nicht bearbeiteten Inhalten. Für Lehrende ist häufig auch die Frage relevant, wieviele Studierende ein Dokument zur Kenntnis genommen haben.
- Nutzungsstatistiken: Erkennen von Nutzungsmustern, in bestimmten Fällen auch die Bewertung der Studierenden.

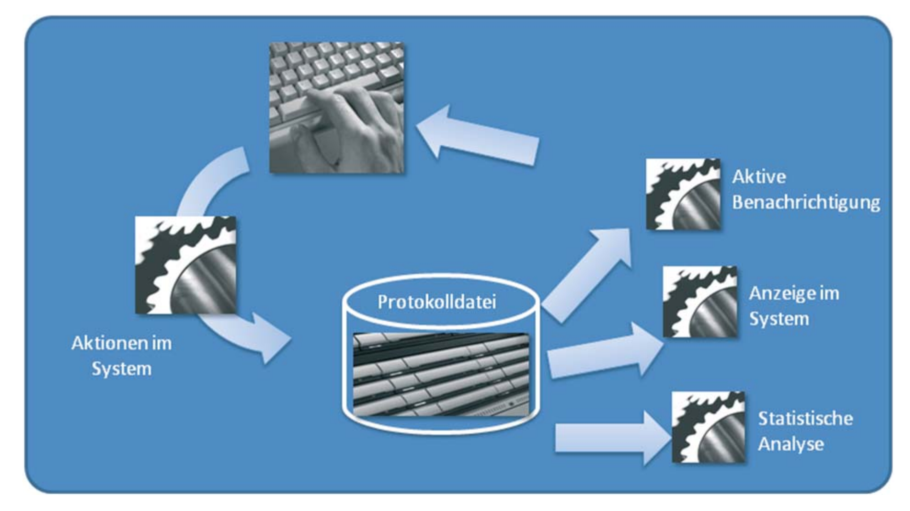


Abbildung 2: Protokolldaten auf Vorrat

Hintergründe dieser Funktionen sind Funktionen, die in Kooperationsumgebungen (Dokumentenmanagement, Groupware, Wissensmanagement) unter dem Stichwort „Group-Awareness“[5] enthalten sind. Kooperationspartner werden durch Systeme darin unterstützt, Veränderungen in der Arbeitsplattform schneller wahrzunehmen. Dabei werden offene und symmetrische Kooperationsbeziehungen vorausgesetzt. Die Diskussion von Datenschutzaspekten ist in der Literatur zu diesen Themen kaum zu finden. Die Übernahme dieser Funktionen ist inhaltlich sinnvoll, teilweise für den praktischen Betrieb auch erforderlich, aber sie bringt natürlich diverse Probleme aus Datenschutzsicht mit sich.

Das Grundkonzept der Implementierung der Funktionen sieht eine Aufzeichnung von Nutzerverhalten zunächst ohne Betrachtung der möglichen oder gar erforderlichen späteren Nutzung vor. Zunächst werden prinzipiell alle Aktionen aufgezeichnet, damit sie für die spätere Verwendung zur Verfügung stehen. Dies ist unabhängig von einer tatsächlichen späteren Nutzung für Benachrichtigungen, Systemanzeigen oder Analysen. Gängig sind hier systemweite Einstellungen. Man kann also in der Systemkonfiguration meist das Logging vollständig abschalten. Diese Lösung würde zwar zu einem rechtlich nicht zu beanstandenden System führen, allerdings würde man dabei auf viele der sinnvollen Funktionen verzichten.

Es stellt sich die Frage, welche Funktionen denn erforderlich sind. Bei der überwiegenden Zahl der Vorlesungen und Veranstaltungen würde man mit einem sehr eingeschränkten Funktionsumfang sehr gut auskommen, bei dem dann auch nur im erforderlichen Umfang Nutzerverhalten erhoben werden dürfte. Allerdings sind die wenigen Veranstaltungen, in denen angepasste didaktische Konzepte erprobt werden, gerade auf die weitergehenden Funktionen angewiesen. Beispielsweise ist es für Studierende sinnvoll direkt zu sehen, was Kommilitonen verändert haben, seitdem man selbst zuletzt in der E-Learning-Plattform aktiv war, wenn das gemeinsame Erarbeiten von Inhalten Teil des didaktischen Konzeptes ist. Für solche Veranstaltungen können Systemfunktionalitäten, die auf Protokollierungen angewiesen sind, erforderlich sein.

Was den Plattformen fehlt, ist eine flexible Konfiguration der Verhaltensaufzeichnung auf verschiedenen Ebenen. Für den weit überwiegenden Teil der Veranstaltungen funktioniert ein Muster, bei dem nur relativ wenige Daten erhoben werden (z.B. Schreibereignisse auf Lehrveranstaltungsdokumentationen), um angemessene Benachrichtigungen umzusetzen. Für wenige Einzelfälle von Lehrveranstaltungen können entsprechend der erforderlichen Funktionalitäten spezifische Protokollinformationen aufgezeichnet werden. Diese könnten in den Hochschulen ein spezielles Kontroll-, Genehmigungs- und Konfigurationsverfahren durchlaufen. Die Stufe der Einstellbarkeit auf Veranstaltungsebene wäre gegenüber dem aktuellen Stand der Systemoptionen bereits ein großer Schritt, jedoch wäre es noch viel wünschenswerter, die gesamte Konfigurierbarkeit so umzustellen, dass sie durch die Nutzung von Funktionen erst ausgelöst wird. Aus Datenschutzsicht ist die Datenerhebung immer vom eigentlichen Zweck ausgehend zu motivieren. Diesem Weg folgend wäre es sinnvoll , erst beim (zulässigen) Einschalten einer (Benachrichtungs-) Funktion die dazu erforderliche Aufzeichnung von Ereignissen einzuschalten. Das sind zunächst erste Ansätze zur Behebung der Probleme. Es sind weitergehende Lösungen vorstellbar, zu deren Realisierung Forschungsbedarf besteht.

Weitere Problembereiche

Die Datenerhebung des Nutzerverhaltens ist sicherlich das offensichtlichste der Datenschutzprobleme in den aktuell zur Verfügung stehenden E-Learning-Plattformen. Allerdings sind auch weitere Problembereiche häufig zu finden:

Mangelndes Identitätsmanagement – Im Gegensatz zu öffentlichen Plattformen sind im E-Learning direkte, unvermittelte Beziehungen vorhanden. Lehrende kennen ihre Studierenden und müssen diese auch kennen, um später

5 Siehe z.B. Chyng-Yang Jang; Charles Steinfeld; Ben Pfaff (2002): Virtual-team awareness and groupware support: an evaluation of the Team SCOPE system. In: International Journal of Human-Computer Studies 56(1). S. 109-126.



Leistungsbewertungen abgeben zu können. In vielen Plattformen findet bei der Anmeldung von Nutzern aber keine wirkliche Identitätsprüfung statt. Als resultierendes Problem können sich Personen im Namen anderer Studierender anmelden und im Namen dieser Personen handeln und diese durch ihr Handeln in Misskredit bei den Lehrenden bringen.

Löschung – Selten sind in den Systemen bereits Überlegungen zu angemessenen Löschkonzepten zu finden. Meist existiert nur die Möglichkeit, selektiv einzelne Beiträge oder aber einen Kurs als Ganzes zu löschen, was häufig dazu führt, dass Daten unnötigerweise lang aufgehoben werden. Verständlicherweise nutzen Lehrende eine vorangegangene Veranstaltung als Basis zur Konfiguration der inhaltsgleichen Folgeveranstaltung. Beispielsweise wären das Anonymisieren von Diskussionsbeiträgen oder das automatische Löschen von Inhaltsbereichen, die nicht wiederverwendet werden sollen, Funktionen, mit denen die datenschutzrechtlichen Löschanforderungen besser erfüllt werden könnten.



Berechtigungskonzepte – Die Berechtigungen zur Einsicht von Daten sind sehr unterschiedlich einstellbar. Die Systeme haben hier meist durchaus weitgehende Konfigurationsmögli chkeiten. Hier liegen die Defizite eher bei der Nutzung durch die Lehrenden. Professoren wollen selbstverständlich der weitreichenden Verantwortlichkeit durch weitgehende Berechtigungen Ausdruck verleihen, obwohl sie tatsächlich selten im System aktiv sind. Stattdessen stellen oftmals studentische Hilfskräfte Dateien ein oder erfassen Ergebnisse von Übungen. Hilfskräfte sollen hingegen möglichst unerkannt bleiben, dürfen aber in der Regel alle Daten einsehen. Obwohl technisch häufig möglich, sind in der Praxis oft Lösungen zu finden, in denen alle Personen oder Rollen, die an der organisatorischen Durchführung beteiligt sind, umfassende Berechtigungen im System zugestanden werden. Problematisch ist dann oft die Konstellation, die sich daraus ergibt, dass studentische Hilfskräfte typischerweise an einem Lehrstuhl in der eigenen Fakultät arbeiten und dann unter den vorgenannten Bedingungen leicht die Möglichkeit haben, die Leistungsdaten von Kommilitonen einzusehen.

Transparenz der Transparenz – Das Problem mit den Berechtigungen wird auch dadurch verschärft, dass in den Systemen für Nutzer nicht transparent ist, wer welche Daten einsehen kann oder gar eingesehen hat. Verlässliche Informationen darüber, wer wann welche Daten einsehen konnte oder es auch getan hat, können auch das Verhalten der Lehrenden für den Datenschutz positiv beeinflussen.

Prüfungsdaten – Zu guter Letzt findet in der Entwicklung derzeit eine enge Integration der Plattformen in die Hochschulprozesse statt. Nach Ansicht der Entwickler und Hersteller sollen die Systeme beispielsweise den Studierenden auch Prüfungsdaten liefern. Da an die Lehr- und Lernplattform in der Regel aber andere (nämlich: geringere) Sicherheitsanforderungen gestellt werden, als dies für sensible Prüfungsdaten erforderlich ist, ist eine solche Koppelung als problematisch zu betrachten.

Fazit

Unter der Geschwindigkeit, mit der E-Learning Plattformen entwickelt werden, hat die Erfüllung von Datenschutzanforderungen sehr gelitten. Insbesondere bei der Protokollierung wäre ein Innehalten und eine grundsätzliche Neukonzeption der Funktionen erforderlich, um selbst grundlegende Datenschutzanforderungen umzusetzen. Stattdessen werden jedoch immer weitere Funktionen, die man im weltweiten Netz an anderen Stellen unter anderen Rahmenbedingungen findet, an die schon jetzt beeindruckenden Systemgebäude angebaut. E-Learning-Systeme stehen dabei nicht nur im Wettbewerb miteinander, sondern auch mit öffentlich erreichbaren Plattformen: So weichen Studierende eher auf Systeme wie StudiVZ (et al.) aus, wenn sie bestimmte Funktionen vermissen oder wenn sich die Bedienung des E-Learning-Systems etwas unkomfortabler darstellt als gewohnt. All dies sollte jedoch nicht dazu führen, stets diesen Plattformen nachzueifern. Stattdessen sollte Vertrauen darin geschaffen werden, dass die Plattformen an den Hochschulen den gestellten rechtlichen Anforderungen gerecht werden und die persönlichen Daten von Studierenden und Lehrenden dort besser aufgehoben sind. Erste Ansätze und Überlegungen für technische Lösungen existieren.[6] Aber bis zur Umsetzung in der Praxis ist es vom jetzigen Stand der E-Learning-Systeme noch ein weiter Weg.

6 siehe Franz, E., Böttcher, A., Wahrig, H., Borcea-Pfitzmann, K.: Access Control in a Privacy-Aware eLearning Environment. In: Proceedings of AReS 2006, Workshop on Security in eLearning (SEL), Vienna, April 2006.

Prof. Dr. Michael Wettern

Lehrevaluation an Hochschulen

Hochschulen sind zur Sicherung und Fortschreibung der Qualität ihres Lehrangebotes verpflichtet, Lehrveranstaltungen in regelmäßigen Abständen zu evaluieren. Dies stellt einen Eingriff in Persönlichkeitsrechte dar, der nicht auf Freiwilligkeit beruhen sollte. Da die Ergebnisse der Lehrevaluation in zunehmendem Maße parametergesteuerte Mittelvergaben begründen, sind die notwendigen Regelungen datenschutzkonform zu gestalten. Dies stellt die behördlichen Datenschutzbeauftragten in den Hochschulen mit ihren begrenzten Einwirkungsmöglichkeiten vor besondere Aufgaben. Der Artikel ist ein Plädoyer dafür, Datenschutz als Qualitätsmerkmal an den Hochschulen öffentlichkeitswirksam zu nutzen.



Einleitung

Die Einführung von Bachelor- und Masterstudiengängen hat die bundesrepublikanischen Hochschulen für den europäischen Bildungsmarkt geöffnet. Um der damit verbundenen, deutlich verstärkten und länderübergreifenden Konkurrenzsituation zwischen den Hochschulen erfolgreich begegnen zu können, nutzen die Hochschulen seit dieser Zeit nahezu flächendeckend Instrumentarien zur Optimierung der ihnen übertragenen Aufgaben.

Externe Gutachter urteilen über die Qualität von Forschung und Lehre in Fachbereichen/Fakultäten und Studiengänge werden vor der Einführung von Bachelor- und Masterabschlüssen einer Evaluation unterzogen. Diese Evaluationen müssen zukünftig zur Qualitätssicherung und –entwicklung wiederholt durchgeführt werden. Verlängerungen von Juniorprofessuren und Stellen der W-Besoldung werden von erfolgreichen Evaluierungen abhängig gemacht. Hochschulverwaltungen überprüfen die Effektivität ihrer Arbeit, denn sie sollen die Hochschule bei der Durchführung ihrer Aufgaben nach besten Kräften unterstützen. Diese an den Hochschulen seit einigen Jahren etablierten Optimierungen werden nicht mehr wie früher überwiegend in Papierform realisiert, sondern verstärkt durch computerbasierte Verfahren ermöglicht. Die verschiedenen Aspekte von Evaluierungen und Optimierungen, denen sich alle Bereiche der Universitäten stellen müssen, lassen sich in ihrer Fülle nur so in realistischen Zeiträumen umsetzen. In vielen Fällen wird das Lehrpersonal dadurch verstärkt mit neuen Aufgaben betraut, die zusätzlich zu den eigentlichen Tätigkeiten in Forschung und Lehre sowie im Prüfungswesen bewältigt werden müssen.

Die Einführung computergestützter Verfahren zur Personal- und Studierendenbetreuung, einschließlich des Prüfungswesens und der Alumni-Betreuung, der Hörsaalvergabe und der Einführung weiterer sicherheitsrelevanter Techniken, hat in den vergangenen Jahren erheblich neue Anforderungen an den Datenschutz und die Datensicherheit der Hochschulen gestellt. Die Aufgaben der Datenschutzbeauftragten sind damit deutlich gestiegen, die Voraussetzungen ihrer realistischen Umsetzung leider nicht in allen Fällen in gleichem Maße.

Studierende werden bei diesen Evaluationen insofern eingebunden, als sie per Landeshochschulgesetze ausdrücklich zu Meinungsäußerungen zu den von ihnen besuchten Lehrveranstaltungen befragt werden sollen.

So forderte das Niedersächsische Hochschulgesetz (NHG) in der Fassung vom 24.6. 2002 in § 5, Studierenden am Ende eines jeden Semesters die Möglichkeit zur Lehrevaluation zu geben. Das novellierte NHG (in der Fassung vom 26.2.2007) hat die Verpflichtung zur Lehrevaluation auf einmal pro Jahr reduziert. Dabei steht es den Hochschulen nicht frei, ob sie diese Evaluation anbieten, oder sie nur auf Nachfrage der Studierenden ermöglichen: Der Gesetzgeber hat diese Lehrevaluation zur jährlichen Verpflichtung gemacht. Um den Datenschutz bei diesen Evaluationen zu gewähren, sind laut § 5 NHG in Verbindung mit § 17 NHG Ordnungen notwendig, die sowohl den Inhalt als auch das Instrumentarium sowie weitere Einzelheiten der Durchführung von Lehrevaluationen regeln. Diese Ordnungen sind die Grundlage, nach der die Lehrevaluationen nicht von der freiwilligen Zustimmung der betroffenen Lehrenden abhängen, sondern die Teilnahme an dem Verfahren zur Qualitätssicherung durch die Hochschulen verpflichtend ist.

Musterordnung

Um den niedersächsischen Hochschulen die Durchführung der Lehrevaluation zu erleichtern, wurde durch eine interministerielle Arbeitsgruppe eine „Musterordnung zur internen Evaluation an Hochschulen in Niedersachsen“ erarbeitet und im Dezember 2003 veröffentlicht[1] (in Anlehnung an bereits geleistete Arbeiten in anderen Bundesländern[2]). Ziel dieser Musterordnung ist es, bei der Realisierung der Lehrevaluation an den einzelnen Hochschulen als „Leitplanke“ zu dienen und damit die Umsetzungen in den einzelnen Hochschulen zu erleichtern. Verschiedene niedersächsische Hochschulen haben das Angebot genutzt, wie das Ergebnis einer Umfrage unter den Datenschutzbeauftragten der Hochschulen ergab. Bei anderen

1 http://www.tu-braunschweig.de/datenschutz/aktuell.

2 Beispielsweise: Evaluationsordnung der Bergischen Universität – Gesamthochschule Wuppertal vom 23.09.2002 (https://bscw.uni-wuppertal.de/pub/bscw.cgi/d79645/Eva_Ordnung.pdf); 31. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, vorgelegt zum 31.12.2002, Punkt 14.1.2; Mustersatzung zur Evaluation an Hochschulen (http://www.datenschutz.hessen.de/Tb31/K25P05.htm).

Hochschulen scheiterte die Umsetzung häufig an der Unfähigkeit, einen Konsens über den in Lehrevaluationen zu verwendenden Fragenkatalog erzielen zu können.

Selbstverständlich unterscheiden sich die rechtlichen Grundlagen der Lehrevaluationen von Bundesland zu Bundesland. Das Berliner Hochschulgesetz fordert in seinem § 6b zur „Evaluation von Forschung und Studium“ eine Satzungsregelung, die von den einzelnen Hochschulen bis zum 31. Dezember 2006 hätte erlassen werden müssen. Das scheint bis auf den heutigen Tag an keiner Hochschule Berlins realisiert zu sein. Dabei orientieren sich Lehrevaluationen durchaus an fundierten Empfehlungen (beispielsweise der Hochschulrektoren-Konferenz), in verschiedenen Fällen sind zur Durchführung dieser Evaluationen an den Hochschulen eigens mit der Koordinierung beauftragte Stellen eingerichtet worden und für die Verfahren werden auch moderne computergestützte Programme genutzt. Aber dennoch fehlt allen Lehrevaluationen an Berliner Hochschulen die Erlaubnisgrundlage in Form einer Satzung. Die Lehrevaluationen werden, sofern sie überhaupt stattfinden, ausschließlich auf der Freiwilligkeit aller beteiligter Personen (Lehrende und Studierende) beruhend durchgeführt. Wegen der fehlenden Verordnung können sie jedoch nicht einheitlich nach vorher festgelegten Regeln erfolgen.



Persönlichkeitsrechte

Legale Eingriffe in die Persönlichkeitsrechte des Einzelnen erlauben die Datenschutzgesetze auf unterschiedlichen Wegen: durch spezielle gesetzliche Vorgaben (zu denen Gesetze, ministerielle Runderlasse aber auch hochschuleigene Ordnungen/Satzungen und Richtlinien zählen) und durch die Einwilligung der Betroffenen. Als Datenverarbeitung ist durch den Gesetzgeber das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen personenbezogener Daten definiert.[3] Dabei unterliegt die Verarbeitung der Daten einer Zweckbindung und sie sind sparsam zu verarbeiten (Datenaskese). Auf diesen rechtlichen Grundlagen müssen die Hochschulen die für eine Lehrevaluation notwendigen Inhalte und einzelnen Arbeitsschritte festlegen.

Das Bundesverfassungsgericht hat in seinem Urteil zur Volkszählung 1983 nicht nur die informationelle Selbstbestimmung ausdrücklich als Grundrecht anerkannt. Es hob auch hervor, dass im Mittelpunkt der grundgesetzlichen Ordnung Wert und Würde einer Person stehen, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient - neben speziellen Freiheitsverbürgungen - das in Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht, das gerade auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit Bedeutung gewinnen kann.[4] Damit kann die informationelle Selbstbestimmung als eine Grundvoraussetzung einer demokratischen Gesellschaft bezeichnet werden. Ein auf das Individuum bezogenes Verständnis von Datenschutz kann aber nur bei gleichzeitigem Bewusstsein von Privatheit bestehen. Dies jedoch scheint in wachsendem Masse verloren zu gehen oder vielfach bereits nicht mehr vorhanden zu sein.[5] Bei dem zu beobachtend ausgeprägten „elektronischem Exhibitionismus“[6] werden bisweilen Stimmen laut, die freiwillige Zustimmung als Rechtsgrundlage der Verarbeitung personenbezogener Daten zu streichen.[7] Denkbar wäre dies auch im Falle von Hochschulen anzuwenden, da diesem Bereich weitgehend die Vertragsfreiheit fehlt.[8] Eine unüberschaubare Anzahl von Studierenden wurde der Studienplatz zugewiesen, der Studienort war nicht ihre freie Wahl. Sofern dennoch einzig eine auf Zustimmung beruhende Verarbeitung von Studierendendaten angestrebt wird, müssen mehrere Alternativen angeboten werden. Nur so werden Einzelpersonen nicht ihrer freien Selbstbestimmung beraubt und zum Gegenstand fremder Willensausübung und Kontrolle. Das Bundesverfassungsgericht hat in seinem Urteil zur Volkszählung 1983 jedoch festgehalten, dass Personen in freier Selbstbestimmung wählen. Das beinhaltet einerseits Möglichkeiten der Wahl zwischen Alternativen und andererseits umfasst es auch, von dem Wahlrecht kein Gebrauch zu machen.

Festlegungen zur Lehrevaluation

Die vorstehenden Erläuterungen machen es deutlich, dass Lehrevaluationen durch Hochschulordnungen/Satzungen/Richtlinien zu regeln und nachstehende Inhalte festzulegen sind:

1. Geltungsbereich.
2. Bewertungsverfahren.
3. Zweckbindung der Daten (beispielsweise: Nutzung zur Vorbereitung von Entscheidungen durch hochschulinterne Organe und Gremien; Verwendung bei Aufsichts- oder Steuerungsfunktionen; zu Zwecken der Ressourcenzuteilung sowie zur Rechenschaftslegung der Hochschule gegenüber der Öffentlichkeit).
4. Festlegung der zu erhebenden personenbezogenen Daten (beispielsweise: studienbezogene und lehrbezogene Daten; Daten zum wissenschaftlichen und künstlerischen Nachwuchs; forschungsbezogene Daten); es empfiehlt sich, eine Aufstellung aller denkbar

3 § 3, Absatz 2 Niedersächsisches Datenschutzgesetz (Nds. GVBl. S. 634), siehe auch unter http://www.lfd.niedersachsen.de/master/C27792_L20_D0_I560_h1.html

4 BVerfGE 65, 1 – Volkszählung, siehe unter http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm

5 Schaar, P. (2007) Das Ende der Privatsphäre, C. Bertelsmann, ISBN 978-3-570-00993-2

6 Hamann, G. (2007) Meine Daten sind frei, DIE ZEIT Nr. 45, 1. November

7 Pötzel N.F. (2007) Einfallstor in die Privatsphäre, Spiegel Special 3/2007, S. 57

8 Wettern, M. und von Knop, J. (2004) Datenschutz im Hochschulbereich, Jahrbuch der Heinrich-Heine-Universität Düsseldorf, S. 575-589.

notwendigen Daten zu erstellen, die für zukünftige Evaluierungen genutzt werden können.
5. Beachtung der Datensparsamkeit.
6. Behandeln Gremien nicht anonymisierte Daten, so hat dies in nichtöffentlicher Sitzung zu erfolgen; alle Beteiligten sind vorher nachdrücklich auf das Datengeheimnis der Landesdatenschutzgesetze zu verweisen.
7. Festlegung des Instrumentariums der Verarbeitung.
8. Frühestmögliche Anonymisierung der Daten von den an der Evaluation beteiligten Studierenden; Sicherstellung, dass nur Studierende eine Lehrveranstaltung bewerten, die diese auch kontinuierlich besucht haben.
9. Festlegung des Verbleibs der erhobenen Daten.
10. Festlegung der mit der Durchführung der Evaluation betrauten Personen und deren Verantwortlichkeit und damit auch der Einhaltung datenschutzrechtlicher Vorschriften.
11. Regelung der Veröffentlichung und Weitergabe der Ergebnisse: hochschulintern, extern.
12. Löschung der Daten.
13. Archivrechtliche Vorschriften.



Verfahren der Lehrevaluation

Die ersten Lehrevaluationen wurden häufig mit dem Kostenargument in Papierform und die notwendigen Auswertungen manuell durchgeführt. Für diese Form der Datenverarbeitung sprechen zwar die wesentlich besseren Rücklaufquoten, ein enormer Nachteil ist allerdings, und dies insbesondere in den so genannten Massenfächern, die sich anschließende statistische Auswertung. Diese ist bei komplett manueller Bearbeitung nur schwer zu leisten. Daher haben sich umgehend computergestützte Verfahren etabliert. Als vorteilhaft haben sich die Verfahren erwiesen, bei denen sich papiergebundene Formen mit webbasierten Anwendungen kombinieren lassen. So können nicht nur die webbasierten Versionen der Fragebögen, sondern auch die Papierform der beantworteten Fragebögen nach dem Einlesen und der damit verbundenen Digitalisierung mittels Computer in vielfältiger Art und Weise ausgewertet werden.

Öffentliche Institutionen, die im pädagogischen Bereich tätig sind, können sich kostenlos des Programms für Befragungsprojekte, GrafStat, bedienen.[9] Das Programm darf ausschließlich in öffentlichen Bildungseinrichtungen genutzt und nicht ohne Zustimmung des Autors vervielfältigt oder auf andere Weise weitergereicht werden. Der kommerzielle Einsatz ist ausdrücklich untersagt.

Andere Programme, wie beispielsweise „Zensus"[10], sind käuflich zu erwerben. Diese Softwarepakete bieten im besten Fall Unterstützungen an, um in komplexen Umgebungen, wie dies für Hochschulen typisch ist, kontinuierlich Lehrevaluationen – aber auch jede andere Art von Befragungen – automatisiert und mit geringem Personalaufwand durchführen zu können.

Wie eingangs erwähnt, müssen sich Hochschulen in regelmäßigen Abständen Qualitätsüberprüfungen ihrer Forschung, Lehre aber auch ihrer Verwaltung stellen. Um dem damit verbundenen wiederkehrenden Kostendruck zu reduzieren, werden gegenwärtig Verfahren ersonnen, um die unterschiedlichen Evaluierungen zusammenzufassen und damit zu optimieren. Zu diesen „System-Akkreditierungen" hat der „Deutsche Akkreditierungsrat"[11] Verfahrensregeln erarbeitet, die voraussichtlich ab dem 1. Januar 2008 in Kraft treten. Danach können Hochschulen einen Antrag an den Akkreditierungsrat stellen, zukünftig selbständig System-Akkreditierungen (und damit keine Programm-Akkreditierungen einzelner Bereiche) ihrer Einrichtung insgesamt durchzuführen und dadurch unabhängig von externen Begutachtungen zu werden. Dies setzt allerdings ein funktionsfähiges Qualitätsmanagement der beantragenden Hochschule voraus.

Institutionelles Qualitätsmanagement (IQ)

So hat die Landeshochschulkonferenz Niedersachsen und das Niedersächsische Ministerium für Wissenschaft und Kultur (MWK) mit der ZEvA (Zentrale Evaluations- und Akkreditierungsagentur, Hannover) vereinbart, die bisherige periodische Evaluation der Studienfächer an den niedersächsischen Hochschulen durch eine Evaluation des „institutionellen Qualitätsmanagements" (IQ[12]) zu ersetzen. Für diesen Zweck entwickelte die ZEvA in Zusammenarbeit mit einigen niedersächsischen Hochschulen einen Leitfaden, der gegenwärtig in einem Pilotprojekt umgesetzt wird. Die beiden ersten Pilothochschulen für dieses Vorhaben sind die Technische Universität Braunschweig und die Fachhochschule Braunschweig/Wolfenbüttel. Die Evaluation des IQ ist so angelegt, dass sie verschiedenen Kriterien genügt („Standards and Guidelines for Quality Assurance in the European Higher Education Area", „Code of Good Practice").

Das IQ-Verfahren besteht aus den folgenden einzelnen Verfahrensschritten:

- Selbstbericht
- Vor-Ort-Begutachtung
- Ausarbeitung des Gutachtens
- Stellungnahme der Hochschule und „Follow-up"
- Kriterien für das Qualitätsmanagement in Lehre und Studium.

Als Kriterien bei der Überprüfung wurden formuliert:

- Strategisches Konzept
- Qualitätskultur
- Evaluation der Studienprogramme
- Beteiligung aller „stakeholder"

9 Siehe bei der „Bundeszentrale für politische Bildung" unter der URL http://www.bpb.de/methodik/V6QAM7,0,0,Einf%FChrung_in_GrafStat.html.

10 „Uni Zensus, Komplettlösung zur Lehrevaluation", siehe unter der URL http://www.blubbsoft.de.

11 http://www.dar.bam.de/; http://www.akkreditierungsrat.de.

12 Siehe bei der ZEvA unter der URL http://www.zeva.uni-hannover.de/aktuell/news_InstEv.htm.

- Qualitätssicherung der unmittelbar studienrelevanten Betreuungsleistungen
- Qualitätssicherung der mittelbar studienrelevanten Betreuungsleistungen
- Internationalisierungsstrategie
- Elektronische Medienunterstützung
- Vollständiges und nutzbares Studienangebot
- Prüfungswesen/Evaluation von Studienleistungen und Lernfortschritten
- Lehrveranstaltungsevaluation
- Lehr- und Prüfungskompetenz des wissenschaftlichen Personals
- „Data Warehousing“, Information der Öffentlichkeit.

Die vorstehende Auflistung macht deutlich, dass die Evaluation der Lehre als ein unverzichtbares Element des IQ-Verfahren gesehen wird. Die Ergebnisse der Lehr-Begutachtung lassen sich von den Antworten zu folgenden Fragen ableiten:

1. Finden flächendeckend Lehrveranstaltungsevaluationen statt? In welchen Zeitintervallen? Differenzieren die Fragebögen nach Lehrveranstaltungstypen? Sind sie nach den fachlichen Regeln für die Konstruktion von Fragebögen erstellt und getestet worden? Durch wen werden sie ausgewertet?
2. Wie wird die Durchführung der Befragungen mit anschließender Besprechung der Ergebnisse kontrolliert?
3. Findet eine periodische Auswertung der Evaluationsergebnisse durch die Lehreinheit oder die Fakultät statt?
4. Gibt es ein Verfahren zur Durchsetzung erforderlicher Veränderungen?
5. Werden periodisch zusammenfassende Berichte über festgestellte Mängel und ergriffene oder geplante Maßnahmen veröffentlicht?
6. Welche Erfahrungen hat die Hochschule bisher mit diesem Instrument gemacht? Welche Maßnahmen sind geplant?



Einige und nicht nur niedersächsische Hochschulen, so ist zu befürchten, werden bei der Beantwortung dieser Fragen einen gravierenden Nachholbedarf offenbaren. Diese Defizite werden zukünftig mit den angestrebten System-Verfahren hoffentlich rasch behoben werden. Andere Agenturen, wie beispielsweise die „Akkreditierungsagentur für Studiengänge der Ingenieurwissenschaften, der Informatik, der Naturwissenschaften und der Mathematik e.V.“ sind mit ähnlichen Verfahren einer integrierten System-Optimierung befasst.[13]

Da die Ergebnisse von Lehrevaluationen in Zielvereinbarungen zur Qualitätssicherung und damit in indikatorgestützte Mittelvergaben einfließen (können), sollten die gesetzlich geforderten Evaluationen unter strikter Einhaltung des Datenschutzes durchgeführt werden.

Von besonderer datenschutzrechtlicher Relevanz dabei sind die folgenden Aspekte:

- Bestimmungen über den zu evaluierenden Personenkreis
- Inhalt und Umfang der Auskunftspflicht
- Erhebungsmerkmale
- Erhebungsverfahren
- Bewertungskriterien
- Schlussfolgerungen aus den Bewertungsergebnissen
- Art und Umfang der Veröffentlichung.

Datenschutz und Lehrevaluation

Es ist verständlich, dass Zustimmungen zu diesen Evaluationen nur handwerklich sauber erarbeitete, datenschutzkonforme Hochschulordnungen bewirken können. Lehrevaluationen dienen keinem Selbstzweck, sie sollen die Qualität der Lehre sichern und nicht repressiv gegen Lehrende eingesetzt werden. Solange Evaluationen bei fehlender Hochschulordnung aber unverbindlich, der Verbleib der Daten sowie auch Folgerungen aus den Ergebnissen unverständlich sind, solange können Verbesserungen der Lehre nicht oder nur punktuell gelingen. Diese Art der Qualitätssicherung bewirkt eher eine allgemeine Verunsicherung und kann vorhandene Ablehnungen zum Verfahren deutlich verstärken. Zusammenfassend muss heute immer noch festgehalten werden, dass in Hochschulen der Datenschutz häufig repressiv und kontrollierend eingesetzt und daher auch so beurteilt wird, was leicht Akzeptanzprobleme und Anwendungsschwierigkeiten verursacht. Er wird seltener als Instrument verstanden, das frühzeitig eingesetzt, zur Klärung von Verantwortlichkeiten, zur Gewährleistung von Gesetzeskonformität und zum Ausgleich von Interessen beiträgt.[14]

Einflussmöglichkeiten behördlicher Datenschutzbeauftragter

Den Datenschutzbeauftragten in den Hochschulen stehen nur beschränkte Einwirkungsmöglichkeiten zur Gewährung des Datenschutzes in den Einrichtungen zur Verfügung. So sollten sie bereits in die Planung neuer datenschutzrelevanter Verfahren vor deren Realisierung eingebunden werden. Sie üben beratende Funktionen aus, unterstützen alle an der Hochschule Tätigen bei deren Bemühungen, den Datenschutz einzuhalten. Zur Erfüllung der ihnen zugedachten Aufgaben stehen ihnen jedoch keine wirksamen Einwirkungsbefugnisse zur Verfügung. So fehlen ihnen Sanktionsmöglichkeiten, sie können nur ständig auf die Missachtung datenschutzrechtlicher Vorgaben hinweisen und auf die Einhaltung des Datenschutzes drängen. Bevor der Gesetzgeber diese Aufgaben nicht im Sinne des Datenschutzes geregelt hat, werden die Datenschutzbeauftragten gegen ihren Willen nicht selten in die Rolle von „zahnlosen Papiertigern“ gedrängt.[15]

---

13 http://www.asiin.de/deutsch/newdesign/index_ex5.html.

14 Wettern, M. und J. von Knop (2004) Datenschutz im Hochschulbereich. In: Jahrbuch der Heinrich-Heine-Universität Düsseldorf, A. Labisch (Hrgs.), H. Süssmuth (Konzept. u. Redakt.), WAZ-Druck, Duisburg, IS 3-9808514-3-5, S. 575-589; Wettern, M. (2006) Schutz von Studierenden-Daten, Recht der Datenverarbeitung, Heft 1, S. 14-18.

15 Pahlen-Brandt, I. (2007) Sind Datenschutzbeauftragte zahnlose Papiertiger? DuD 31, S. 24-28.

Datenschutz als Qualitätsmerkmal

So sollten Hochschulleitungen lernen, mit dem Hinweis auf den Datenschutz Eigenwerbung zu betreiben, wie dies Firmen seit Jahren in immer stärkerem Umfang zur Kundenbindung durchführen.[16] In vielen Hochschulbereichen ist leider eine sträfliche Missachtung des Datenschutzes zu konstatieren. Dies trifft auf die vorstehenden Ausführungen zur Lehrevaluation zu wie auch auf die fortgesetzte Speicherung von Daten der Studierenden nach deren Exmatrikulation, wie sie an vielen Hochschulen üblich ist. Nach einer Exmatrikulation sind unter Beachtung von Aufbewahrungsfristen verschiedene Daten (diese auch noch für einen unterschiedlich langen Zeitraum) zu speichern. Andere Daten dagegen, deren Zweckbindungen entfallen sind und für die keine Aufbewahrungsfristen bestehen, sind mit der Exmatrikulation zu löschen, entweder automatisiert oder manuell. In den meisten Fällen werden die nicht mehr benötigten Daten jedoch nicht gelöscht, sondern sie werden schlicht weiterhin gespeichert. Diese permanenten Verletzungen des Grundrechts der informationellen Selbstbestimmung bei der Verarbeitung personenbezogener Daten von Studierenden durch die Hochschulen sind mit allem Nachdruck zu missbilligen. Mit diesem Verhalten missachten die Hochschulen wiederholt und dies seit Jahren das Grundrecht der informationellen Selbstbestimmung. Um die Einhaltung dieses Grundrechts zu gewährleisten, plädiert der Autor dafür, Verstöße dagegen zukünftig mit empfindlichen Strafen zu belegen.[17] Hilfreich wäre in diesem Zusammenhang auch eine deutliche Unterstützung durch die für die Hochschulen zuständigen übergeordneten Fachministerien: Diese sollten zukünftig ihre Aufsichtspflicht auf die Einhaltung des Datenschutzes der von ihnen erlassenen Gesetze ausweiten. Die Nichtbeachtung des informationellen Selbstbestimmungsrechts ist kein Kavaliersdelikt, sondern untergräbt ein die Demokratie sicherndes Grundrecht.

16 Schmundt, H. (2005) Kuschelkurs mit Datenschützern, Der Spiegel, Heft 50, S. 163.

17 Siehe dazu: „Grundrechte-Report 2007 – Zur Lage der Bürger- und Menschenrechte in Deutschland“, T. Müller-Heidelberg et al. (Hrgs.) Fischer Taschenbuch Verlag, Frankfurt am Main, ISBN 978-3-596-17504-8, S. 125.

Sören Jungjohann

„Du hast keine Freunde“ – Meine Reise nach StudiVZ

Online-Netzwerke interessieren mich nicht. Second Life? XING? Facebook? Diese FKK-Kolonien des Internets sind nicht nach meinem Geschmack. Ein Hype jagt den nächsten, und was heute das *next big thing* ist, ist morgen schon Schnee von gestern. Meine knapp bemessene Zeit vergeude ich nicht mit solchen Dingen. Im Internet genügen mir die Nachrichten auf tagesschau.de und der tägliche „Zeit“-Newsletter. Freundschaften pflege ich in der wirklichen Welt.

Irgendwann lese ich von StudiVZ. Die ersten Zeitungsartikel über dieses neue soziale Web-Netzwerk überblättere ich noch achtlos. Das mag am Namen liegen, der an Kindergartensprache und Bundeswehrjargon erinnert. Beides ist nicht mein Ding. Dann die Meldung: StudiVZ hat fast fünf Millionen Nutzer. Mit über 5,3 Milliarden Seitenaufrufen pro Monat steht die Website www.studivz.net auf Platz 1 der deutschen IVW-Rangliste. Unmittelbar danach folgt der „kleine Bruder“ SchülerVZ. Meine Lieblingsseite Heise online rangiert mit 0,1 Milliarden Aufrufen abgeschlagen auf Platz 24.

Ich komme ins Grübeln, informiere mich, hake nach. Die schiere Größe dieses Netzwerks kann kein Zufall sein. Verpasse ich vielleicht etwas? Rollt da ein Zug in das studentische Internetparadies, auf den ich aufspringen sollte?

Der Dienst soll kostenlos sein. Was habe ich zu verlieren? Ich starte den Webbrowser und steuere die Seite www.studivz.net an. Mein erster Eindruck: Das ist aber bieder! Die Website ist schlicht, fast unauffällig. Statt poppiger Farben überwiegen dezente Rottöne. „Bist Du schon drin?“ werde ich gefragt. Nein, noch nicht. Aber gleich. Ich immatrikuliere mich. Etwas bin ich

StudiVZ (Abk. für Studierenden-Verzeichnis) ist eine so genannte *social software*, die sich vornehmlich an Studenten wendet. Vorbild ist das amerikanische Online-Netzwerk Facebook. StudiVZ ermöglicht es seinen Mitgliedern, detaillierte Profile anzulegen und diese mit den Profilen anderer Nutzer zu verbinden. Nutzer mit gemeinsamen Interessen können sich in Gruppen zusammenschließen. Damit bildet StudiVZ (zumindest teilweise) die Vorlieben und die sozialen Netzwerke seiner Mitglieder ab. Seit der Gründung im Jahr 2005 haben sich etwa fünf Millionen Menschen registriert. Hinter StudiVZ steht der deutsche Holtzbrinck-Konzern (Handelsblatt, Die Zeit, Droemer Knaur, Rowohlt u. a.).

überrascht, dass StudiVZ verhältnismäßig wenig Informationen einfordert: Name, Geburtstag, Geschlecht, E-Mail-Adresse und Hochschule. Keine Fragen nach Adresse, Telefonnummer oder sexuellen Vorlieben. Datensammelwut sieht anders aus.

Vor dem endgültigen Immatrikulations-Klick werfe ich noch rasch einen Blick in die Allgemeinen Geschäftsbedingungen (elf Seiten) und die Datenschutzerklärung (noch mal vier Seiten). Beide sind verständlich formuliert und machen einen vernünftigen Eindruck. Da habe ich schon ganz andere Sachen gelesen. Ich habe jedenfalls nicht das Gefühl, mit juristisch fragwürdigen Klauseln über den Tisch gezogen zu werden. (Die kritischen Anmerkungen von Spiegel online zu den AGB[1] lese ich erst Tage später.)

Kurz darauf bin ich mittendrin im Online-Studiverzeichnis. Ich befinde mich auf meiner personalisierten Startseite, die derzeit noch ziemlich öde ausschaut. Interessanter als die Startseite sind die Hyperlinks zu drei (zufällig ausgewählten) Kommilitonen meiner Uni, die mich zum Anklicken verleiten. Ich lande auf der Startseite von Michaela[2], geboren am 03.06.1986, die auf der Suche nach netten Leuten ist, Musik der Sportfreunde Stiller hört und sich selbst als unpolitisch einstuft. „Du hast keine gemeinsamen Freunde mit Michaela“ informiert mich StudiVZ. Macht nichts, ich habe ohnehin schon auf das nächste Foto geklickt und bin nun bei Andreas (Ziegenbart, Heavy-Metal-T-Shirt und halbvolles Bierglas in der Hand). Andreas geizt mit Beschreibungen zu seiner Person. Kein Wort zu Musikgeschmack, Beziehungsstatus und politischer Einstellung. Wurzelt dieses beredte Schweigen in einem vertieften Datenschutzverständnis? Eher nicht: Andreas beweist in vier Fotogalerien, dass er andere an seinem Privatleben teilhaben lassen möchte. Besonders die Fotoserie „In Norberts Partykeller“ gewährt interessante Einblicke. Ob die dort abgelichteten feiernden Studenten wissen, dass ihre Fotos mehreren Millionen Menschen zugänglich sind? Und was, wenn nicht? Die StudiVZ-AGBs sind in diesem Punkt eindeutig: „Sollen Fotoaufnahmen hochgeladen werden, auf denen neben dem Nutzer selbst noch eine weitere oder mehrere Personen zu erkennen sind, darf sowohl der Upload als auch die Markierung bzw. Verlinkung der Bilddatei nur erfolgen, soweit die Zustimmung des bzw. der Dritten hierzu vorliegt.“

Nach einem kurzen Streifzug durch die Bildgalerie „Wir am Baggersee“ (sechs junge Männer und zwei Kisten Bier) werfe ich noch einen kurzen Blick auf die Gruppen, in denen Andreas Mitglied ist. „Gayromeo“ und „Kein Alkohol ist auch keine Lösung“ fallen mir ins Auge. Ersteres lässt tief blicken, Letzteres soll vermutlich lustig sein. Na ja.

Ich verlasse Andreas‘ Seite und kehre zu meiner eigenen Startseite zurück. Die sieht einfach nur dröge aus, aber ein Foto ist schnell hochgeladen. Einigermaßen seriös blicke ich in die Kamera. Wie ein typischer Student schaue ich aber nicht aus. Egal. Jetzt kommen die persönlichen Daten. Die Felder zur Uni und zum Studium sind bald ausgefüllt. Alles kein Problem, jetzt kann ich mich mit den Leuten aus meinem Studiengang verbinden lassen. Die Kontaktfelder lasse ich trotzdem leer. Was geht die Leute meine Telefonnummer oder meine Privatanschrift an? Die E-Mail-Adresse muss reichen. Auch die Rubrik „Persönliches“ bleibt unausgefüllt. Warum sollte ich meine politische Einstellung offenbaren? Und falls ich meine Hobbys und Interessen angebe, führt das doch nur zu unerwünschter personalisierter Werbung und nervigen E-Mails. Zumindest sieht das die Datenschutzerklärung vor: „Ich willige ein, dass StudiVZ die von mir bei der Registrierung mitgeteilten Daten, die von mir freiwillig innerhalb meines eigenen Profils eingetragenen Daten sowie meine Mitgliedschaft in Gruppen dazu nutzt, um mir gezielt personalisierte Werbung und/ oder besondere Angebote und Services über das StudiVZ-Netzwerk zu präsentieren bzw. präsentieren zu lassen.“ Also lasse ich die meisten Felder frei. Trotzdem oder gerade deshalb bin ich unzufrieden. Meine Seite wirkt trotz Foto und Angaben zu meinem Studium müde und leer.

Ich hangele mich weiter durch die StudiVZ-Menüs: Der nächste Punkt nennt sich „Meine Freunde“. Ein Klick und meine Unzufriedenheit steigert sich ins Unermessliche: „Du hast keine Freunde“ teilt mir StudiVZ mit. Die Botschaft hätte auch lauten können: „Keiner hat dich lieb“. Direkter kann man mich nicht auf mein elektronisches Eremitentum hinweisen. Der soziale Druck steigt an. Kein Mitglied bei StudiVZ zu sein, ist möglicherweise noch eine Frage der Einstellung. Aber Mitglied zu sein und keine Kontakte vorweisen zu können, ist ein echter Offenbarungseid.

Ich kämpfe gegen mein Schicksal an und suche nach mir bekannten Kommilitonen. Einige Viertelstunden später habe ich eine handvoll Leute, die auch bei StudiVZ immatrikuliert sind, um ihre virtuelle Freundschaft ersucht. Es dauert einige Tage, bis mir alle geantwortet und die angetragene Freundschaft bestätigt haben, aber schließlich verfüge auch ich über ein kleines soziales Netz im Studiverzeichnis. Was mir das außer Selbstbestätigung bringt, kann ich aber nicht genau feststellen. Der Nutzen von StudiVZ will sich mir nicht so richtig erschließen. Vielleicht muss ich doch mehr von mir preisgeben, um für andere Studierende interessant zu werden. Aber das möchte ich nicht. Zu groß ist meine Sorge, meine Interessen, Vorlieben, Hobbys und persönliche Daten könnten in falsche Hände geraten.

Dass man als Student auch gut ohne StudiVZ über die Runden kommt, berichtet Spiegel online[3]: Studentin Frauke beging „digitalen Selbstmord“, exmatrikulierte sich und ließ auf StudiVZ 193 Freunde, 906 Nachrichten und 232 Pinnwandeinträge zurück. Zehn Tage später stellt sie fest: „Es ist Jacke wie Hose, ob man noch drin ist oder nicht“.

Für solch ein endgültiges Fazit ist es für mich zu früh. Deshalb an dieser Stelle nur eine Zwischenbilanz: StudiVZ scheint weder ein elektronischer Heilsbringer für einsame Studenten



1 Spiegel online vom 14.12.2007: „Experten kritisieren Schnüffel-Passus von StudiVZ“, http://www.spiegel.de/netzwelt/web/0,1518,523413,00.html.

2 Alle Namen wurden aus Gründen des Persönlichkeitsschutzes geändert. Die beschriebenen Profile wurden pseudonymisiert.

3 Spiegel online vom 03.08.2008: „Mein digitaler Selbstmord“, http://www.spiegel.de/unispiegel/wunderbar/0,1518,532070,00.html

noch ein datenfressendes Monstrum aus Ozeanien zu sein. Wer sich immatrikuliert, wird nicht zwangsweise zum gläsernen Studenten. Jeder Nutzer kann in der Rubrik „Meine Privatsphäre“ sein persönliches Datenschutz-Feintuning betreiben. Und es bleibt auch jedem selbst überlassen, ob er seine politische Überzeugung herausposaunt und aufschlussreiche Selbstporträts präsentiert. Effektiver und moderner kann man informationelle Selbstbestimmung eigentlich nicht praktizieren.

Eines muss jedoch auch dem datenschutzbewussten „Studi“ klar sein: Eine sinnvolle Nutzung dieses Dienstes ist nur möglich, wenn man gewillt ist, die digitalen Hosen herunter zu lassen. Ob dies mit dem persönlichen Verständnis von Privatsphäre noch vereinbar ist, muss jeder für sich selbst entscheiden.

Dr. Thilo Weichert

Geplante Visa-Warndatei verletzt informationelle Selbstbestimmung

Im Ausländerzentralregister (AZR) soll nach dem Willen der CDU-Bundestagsfraktion zur Bekämpfung des Visamissbrauchs durch Schleuser und Menschenhändler eine Einladerdatei eingerichtet werden, in der auch Privatpersonen gespeichert werden, die Ausländer zum Besuch einladen und sich gemäß § 68 Aufenthaltsgesetz (AufenthG) verpflichten, die für diese entstehenden Kosten für den Lebensunterhalt zu übernehmen und evtl. zu erstatten.



Im April 2005 hatte die CDU/CSU-Fraktion als Opposition im Bundestag einen Gesetzentwurf zur Einführung einer Warndatei vorgelegt, in der Verdachtsfälle des Missbrauchs durch Einlader registriert werden sollten. Entsprechende Vorstöße der CDU-Fraktion waren auch schon 1997 und 1999 gescheitert, weil sie keine Mehrheit fanden. Nicht jede Einladung eines ausländischen Staatsangehörigen sollte gespeichert werden, sondern nur Fälle, in denen der Verdacht eines Missbrauchs bestand. In der schwarz-roten Koalitionsvereinbarung 2005 wurde dann vereinbart, eine „Warndatei“ einzurichten, nicht eine „Einlader-Datei“.

Zuvor war die Diskussion um Maßnahmen zur Verhinderung des Einladungsmissbrauchs durch ein Urteil des Landgerichts Köln im Jahr 2004 angeheizt worden, das es als strafmildernd erklärte, dass die „banden- und gewerbsmäßige Schleusung von Ausländern durch eine fehlende Datei der Viel-Einlader begünstigt wurde“. Bald darauf kam es zur sog. Visa-Affäre, in deren Verlauf dem Auswärtigen Amt vorgeworfen wurde, es habe die deutschen Konsulate im Ausland dazu angehalten, allzu großzügig Visa zu erteilen. Kritisiert wurde auch, dass die Speicherung von Daten der Einlader rechtlich nicht vorgesehen war und auch nicht praktiziert wurde. Seit zwei Jahren können die Auslandsvertretungen örtliche Dateien über Viel-Einlader einrichten. Ihnen ist es erlaubt, ihre Einlader-Daten auch im Einzelfall untereinander auszutauschen. Infolge der sog. Visa-Affäre versuchte zunächst die rot-grüne und dann die schwarz-rote Bundesregierung, eine Visa-Warndatei auf europäischer Ebene zu installieren, da Visa eines EU-Mitgliedsstaates zur freien Reise in der gesamten EU berechtigen. Nachdem das Europäische Parlament die weitgehenden deutschen Pläne abgelehnt hat, soll nun doch eine deutsche Datei geschaffen werden.

Die Pläne zur Einlader-Datei wurden vom „Verband Binationaler Familien und Partnerschaften“ kritisiert. Dieser interkulturelle Familienverband zeigte sich beunruhigt darüber, dass anlasslos, d.h. ohne Hinweis auf einen Rechtsmissbrauch Daten gespeichert würden. Binationale und eingewanderte Familien laden regelmäßig Familienangehörige und Verwandte aus visumpflichtigen Staaten ein. Sie leben damit ein Familienmodell, das einer zunehmenden Globalisierung folgt und das längere Trennungen und erhöhte Kosten zur Folge hat. Mit der geplanten Datei würden sie nun generell unter Verdacht gestellt, wenn sie den Kontakt zu ihren Angehörigen pflegen. Der Verband meint, die private Einladungspraxis habe nichts mit organisiertem Menschenhandel zu tun. Die anlasslose Datenspeicherung fördere das Misstrauen gegenüber den Behörden. Es würden gruppenbezogen Daten von unbescholtenen Bürgerinnen und Bürgern gesammelt, um „individuelle tatsächliche Straftäter zu erfassen“, was eine Verletzung des Rechts auf informationelle Selbstbestimmung sei. Betroffen von dieser Datenspeicherung sind nicht nur Privatpersonen, sondern auch mittelständische Betriebe mit weltweiten Kontakten und sogar Sport- und Kulturvereine, die ausländische Kontakte pflegen.

Die geplante Warndatei ist unverhältnismäßig. Über sie würden Einladungen gespeichert, die in den meisten Fällen unproblematisch sind. Selbst die meisten der sog. Vieleinlader sind absolut unverdächtig und handeln ausschließlich im Interesse der Pflege privater, kultureller und wirtschaftlicher Kontakte. Für die Zielsetzung der Missbrauchsbekämpfung ausreichend wäre die Speicherung von solchen Einladern, bei denen ein auf Tatsachen basierender begründeter Verdacht des Missbrauchs besteht. Durch die schon derzeit erfolgende lokale Speicherung bei den einzelnen Auslandsvertretungen können mit geringerem Aufwand die angestrebten Zwecke erreicht werden. Es wurden bis heute keine Untersuchungen vorgelegt, die einen



darüber hinausgehenden Bedarf an einer zentralen Speicherung belegen. Eine allgemeine Einlader-Datei würde dazu führen, dass in einer Vielzahl von Fällen eine unnötige aufwändige Überprüfung erfolgen würde. Die Datei würde umgehend auch von weiteren Behörden genutzt, insbesondere von Sicherheitsbehörden, die mit der Begründung der Bekämpfung von terroristischen Straftaten, Wirtschaftskriminalität und Menschenhandel Zugriff auf diese Datei fordern werden (Rath www.taz.de18.11.2007; PE Verband Binationaler Familien und Partnerschaften 26.11.2007; Dahlkamp/ Latsch Der Spiegel 50/2007, 31; www.netzeitung.de 10.04.2005).

Datenschutznachrichten

Deutsche Datenschutznachrichten

Bund/Länder

Kriminalämter fordern heimliche Wohnungsdurchsuchung und Spähangriff

Die Spitzen von Bundeskriminalamt (BKA) und Landeskriminalämtern (LKÄ) drängten in einem an die Innenminister des Bundes und der Länder gerichteten als vertraulich eingestuften 56seitigen Bericht von Anfang November 2007 nach der Festnahme mehrerer islamistischer Terrorverdächtiger im Sauerland im vorangegangenen September (Operation Alberich) auf eine erhebliche Ausweitung ihrer rechtlichen und finanziellen Möglichkeiten. Der Große Lauschangriff solle durch „eine optische Überwachung“ von Wohnungen mit Videokameras, also einem „großen Spähangriff“ gesetzlich ergänzt werden. Zwar sei ein vom mutmaßlichen Terroristen Fritz G. angemietetes Haus im Sauerland verwanzt gewesen, aber auf Grund „schwer verständlicher Kommunikation“ sei das „Geschehen im Ferienhaus zeitweise unklar“ gewesen. Die Ermittler plädierten zudem für eine Grundgesetzänderung, um eine „verdeckte Durchsuchung inklusive verdeckter Videografie“ von verdächtigen Wohnungen zu erlauben. In den Polizeigesetzen der Länder solle außerdem einheitlich geregelt werden, dass Beamte bereits dann „präventivpolizeilich“ Telefonate abhören können, wenn der Betroffene noch kein Beschuldigter sei. Die Kriminalamtschefs wollen die Beobachtung von Internet-Cafés ausbauen, für die es „einen wesentlich höheren Bedarf an Überwachungstechnik für breitbandige Call-Shops“ gebe. Weil die Verdächtigen um Fritz G. und Daniel S. mehrfach per W-LAN über ungeschützte Anschlüsse von Privatpersonen mit Funktionären der „Islamischen Dschihad Union“ (IJU) in Pakistan kommunizierten, regten die Polizeichefs die bundesweite Beschaffung von sog. W-LAN-Catchern an. Die Geräte, die bislang nur beim BKA sowie in Bayern, Baden-Württemberg und Nordrhein-Westfalen eingesetzt werden, simulieren einen Zugangspunkt fürs Internet und ermöglichen so die Überwachung des Datenverkehrs.



Mit der Vorlage ihres Forderungs-katalogs provozierten die Polizei-behörden Konflikte mit den Verfassungsschutz behörden. Als Konsequenz aus dem Verfahren gegen die IJU sei die „aktive Informationsbeschaffung“ auszubauen, v.a. durch den Einsatz von V-Leuten. Damit wollen die Ermittler in die von Straftaten unabhängige Vorfeldarbeit eindringen, was bisher die Domäne der Geheimdienste ist. Deren Arbeit wird offen kritisiert. Die Nachrichtendienste hätten anfangs nur „sehr zurückhaltend und lückenhaft“ berichtet, weshalb es zu „erheblichen Informationsdefiziten“ bei der Polizei gekommen sei.

Die Forderung nach dem Spähangriff ist nicht neu; zuletzt hat das vier Jahre vorher die CDU/CSU und noch neun Jahre früher die SPD propagiert. Bundesinnenminister Wolfgang Schäuble und andere CDU-Politiker sprachen sich rasch prinzipiell für eine Umsetzung der polizeilichen Wunschliste aus. Dabei betonte Schäuble, dass „eines der fundamentalen Menschenrechte auch das Recht auf Sicherheit ist“. Es müsse alles Mögliche getan werden, um Anschläge zu verhindern. Die BundesbürgerInnen müssten sich „viele Jahre“ auf entsprechende Bedrohungen einstellen. Der niedersächsische Innenminister Uwe Schünemann forderte v.a. eine verdeckte Wohnraumüberwachung und -durchsuchung zur Terrorabwehr: „Bei einer terroristischen Bedrohungslage muss es möglich sein, auch ohne das Wissen der Betroffenen Wohnungen zu durchsuchen.“ Die Gewerkschaft der Polizei (GdP) plädierte auch für die Erweiterung der polizeilichen Ermittlungsmaßnahmen, etwa für die Videoüberwachung von Wohnungen, in denen sich mutmaßliche Schwerkriminelle aufhalten.

Linken-Fraktionsvize Petra Pau rügte dagegen, dass das „BKA wieder ein Attacke gegen das Grundgesetz startet“. Die Polizei sei unersättlich. Der parlamentarische Geschäftsführer der Grünen Volker Beck lehnte Spähangriffe ab: „Es gilt einerseits, die Gefahren ernst zu nehmen, und andererseits, Augenmaß zu behalten und populistischer Panikmache entgegenzuwirken“. Der grüne Geheimdienstexperte Hans-Christian Ströbele warnte, „dass unter dem Trommelfeuer der immer neuen Gesetze von dem Grundrecht auf Unverletzlichkeit der Wohnung und von dem Post- und Fernmeldegeheimnis nicht viel übrig bleibt. Es muss einen Kernbereich der privaten Lebensführung geben, der für den Staat tabu ist“. Der FDP-Innenexperte Max Stadler mo-

nierte, Schäuble beschreite einen „gefährlichen Weg“. Die Grundrechte und der Schutz der Menschenwürde würden eine Schranke bilden, die bei der Gefahrenabwehr nicht überschritten werden dürfe. Der Bundesinnenminister nähere sich in bedenklicher Weise der Lehre vom „Feindstrafrecht“.

Hohe Verfassungsschützer wiesen die Kritik der Polizei an ihrem Verhalten während der Terrorfahndung im Sauerland energisch zurück. Ein Verfassungsschützer, der während der gesamten Zeit in den Fall eingebunden war: „Ausgerechnet diesmal ist alles wirklich ordentlich gelaufen, wir haben wirklich alles, was die Gefährlichkeit betraf und zur Lageeinschätzung diente, zeitnah übergeben. Aber Polizisten verstehen nicht, dass sie nicht alles wissen müssen. Sie werden nie zufrieden sein, was wir ihnen geben.“ Ein anderer hoher Geheimdienstmann: „Das Papier hat bei den Verfassungsschützern bundesweit erheblichen Ärger ausgelöst. Wir geben zu, dass es Schwächen der Information in der Anfangszeit des Falles gab. Aber das lag am Veto der Amerikaner; wir durften deren geheime Informationen nicht einfach an die Polizei weitergeben“. Ein anderer Verfassungsschützer über den Bericht: „Die wollen doch, dass wir am Ende eine Art Bundeszentrale für politische Bildung sind. Das ganze Papier ist reine Propaganda.“ Das BKA solle zu einer Art deutschem FBI aufgewertet werden; die Nachrichtendienste sollten die „Super-Bullen“ allenfalls noch auf die Spur setzen und sich ansonsten ruhig verhalten. „Wir sind aber ein Korrektiv zur Polizei.“ Ein ungenannter hoher Sicherheitsbeamter äußerte gegenüber dem „Focus“ in Bezug auf die im Bericht geforderten in-camera-Verfahren, wonach einzelne Aktenteile „nur für das Gericht einsehbar sein sollen“: „Da steuern wir auf Geheimprozesse zu, die es so nur in Diktaturen gibt.“



Es gibt aus dem Bericht weitere Erkenntnisse aus den Ermittlungen gegen die Terrorverdächtigen im Sauerland. So dauerte es einmal sechs Wochen, bis die Mitschnitte eines vierstündigen Telefongesprächs der Verdächtigen bearbeitet waren, weil es im BKA nur vier Phonetiker gibt, die diese diffizile Arbeit leisten können. Einmal schafften es die Fahnder nicht, schnell geheime Informationen auszutauschen, weil es auf ihren Dienststellen keine Telefone mit Verschlüsselungsmöglichkeiten gab. Während die Bombenbauer in ihrer Wohnung darüber sprachen, wie sie ihre Bombe anfertigen wollten, begann einer der drei Verdächtigen plötzlich zu beten. Die Fahnder meinten daraufhin, die Wanzen abschalten zu müssen. Die schalteten diese aber bald wieder an, weil sie das Gefühl hatten, dass sie durch das Gebet nur ausgetrickst werden sollten (Der Spiegel 50/2007, 18; Krempl www.heise.de 10.12.2007; SZ 10.12.2007, 4, 5; Ramelsberger SZ 12.12.2007, 2 u. 14.12.2007, 6; Musharbash www.spiegel.de 12.12.2007; www.focus.de 15.12.2007; Krempl www.heise.de 18.12.2007).

Bund/USA

Post liefert Briefgeheimnisse an US-Behörden

Die Vereinigten Staaten von Amerika (USA) verlangen Absender- und Empfängerdaten von Briefen und Paketen, die in die USA gesandt werden. Die Post stellt diese Daten teilweise schon zur Verfügung. Die Forderung nach den Daten - wenn vorhanden selbst über den Inhalt - werden schon seit Jahren gestellt. Ziel ist es, Anschläge wie die Versendung von Antrhrax im Jahr 2001 oder von anderen gefährlichen Materialien zu verhindern. Zudem möchte das US-Heimatschutzministerium postalische Kontakte zwischen Terrorverdächtigen aufspüren. Bislang hat sich in der Europäischen Union (EU) nur Österreich gegen die Weitergabe der Postdaten gewehrt, so Michael Homolla, Sprecher der Österreichischen Post: „Schließlich würde dies dem Postgeheimnis widersprechen, wonach Daten über Sendungen nur an Absender oder Empfänger mitgeteilt werden dürfen“.

Derzeit finden geheime Verhandlungen über den Postdaten-Austausch statt, deren Ziel es ist, alle Staaten auf einen einheitlichen - nämlich den amerikanischen - Standard zu verpflichten. Die amerikanische Zoll- und Grenzbehörde CBP (Customs and Border Protection) verlangt bisher bei Express-Paketen die elektronische Bereitstellung der Kundendaten noch vor dem Eintreffen in den USA. Vier Stunden vor den Landung des Transportflugzeugs müssen die Daten den US-Behörden vorliegen. Ein Handelsabkommen (Trade Act) mit der EU von 2004 sieht vor, dass diese Daten auch an Strafverfolgungsbehörden weitergegeben werden und mit kommerziellen Datenbanken abgeglichen werden dürfen. Dieser Regelung unterliegen grundsätzlich auch, so das sog. Advanced Air Manifest, Briefe. Für die Umsetzung wäre eigentlich ein Beschluss des Weltpostvereins nötig, den es aber bislang nicht gibt.

Die Posttochter DHL liefert die Daten bei Expresssendungen bereits, dazu auch die Zollinhaltsangabe, die auf den Pakteten gemacht werden muss. DHL, ursprünglich eine US-amerikanische Firma, hat Sitze in den USA und in Deutschland. Derart werden amerikanische Gesetze auf Deutschland ausgedehnt. Die USA müssen gar nicht offiziell anfragen. Gemäß dem Sprecher der Deutschen Post World Net genügt eine Veröffentlichung in den „einschlägigen Medien“ als Grundlage für die Datenweitergabe. Die Deutsche Post erledige nur einen Job für ihre Kunden. Von der Übermittlung der Postdaten an die US-Behörden wissen aber allenfalls große Unternehmen und sonstige Großkunden. Privatleute, die Pakete oder Päckchen per DHL über den Atlantik schicken, wissen davon regelmäßig nichts.

Zu den Gesprächen über eine Ausweitung des Datenaustauschs konnte oder wollte sich ein Vertreter der Deutschen Post - wegen der „Schwierigkeit der Materie“ - nicht äußern. Die Bundesregierung wollte nicht mitteilen, wer für die deutsche Seite die Gespräche führt. Das Auswärtige Amt ließ mitteilen, in der Angelegenheit sei das Bundesinnenministerium zuständig. Das verwies auf das Bundeswirtschaftsministerium. Dort erklärte eine Sprecherin, ihr Haus sei nur im Rahmen des Weltpostvereins damit befasst: „Das Thema Postdatenübermittlung wird in unterschiedlichen Gremien erörtert.“ Andreas Hach vom österreichischen Verkehrsministerium in Wien versprach, standhaft zu bleiben. In den



USA entsteht mit Hilfe der aus Europa gelieferten Informationen eine gewaltige Datenbank, über die genau verfolgt werden kann, wer wem was wann geschickt oder geschrieben hat. Ein hochrangiger deutscher Datenschützer: „Dem amerikanischen Zoll kann doch nichts Besseres passieren, als dass er erfährt, wer an wen eine interessante Sendung schickt, die es vielleicht lohnt zu öffnen, zum Beispiel, weil Konstruktionszeichnungen darin sind". Es bestehe die Gefahr, dass Unschuldige kriminalisiert würden. Ein Sprecher des Bundesbeauftragten für den Datenschutz und Informationsfreiheit (BfDI) Peter Schaar sagte dagegen auf Anfrage, man habe sich „von der Post erläutern lassen, wie der Sachstand ist". Danach bestünden aus Datenschutzsicht keine Bedenken. Für weiter gehende Fragen verwies der BfDI auf den, den er kontrollieren soll: die Post.

Diese stellte klar, dass für Briefe und normale Postpakete in die USA der Weltpostvertrag gilt. Nicht von diesem Vertrag erfasst würden sog. Express-Sendungen. Derartige Versendungen erfolgen durch DHL Express, FedEx, UPS oder TNT. Im Rahmen des seit Dezember 2003 in Kraft befindlichen Trade Acts 2002 der USA bestehe die Pflicht, elektronische Informationen über Warentransporte bei Einfuhren in die USA der zuständigen Zollbehörde vor Ankunft der Waren zur Verfügung zu stellen. Der Zeitrahmen ist nach dem Advanced Manifest System (AMS) abhängig vom jeweiligen Verkehrsweg; beim Luftverkehr ist eine Information vier Stunden vor Landung des Flugzeugs in den USA Pflicht. Die Umsetzung des Trade Act auf Sendungen nach dem Weltpostvertrag sei bisher ausgesetzt worden., so dass derzeit in der Praxis noch keine Daten übermittelt würden. Die Deutsche Post übermittele, wie seit Jahren international üblich, die erforderlichen Zolldokumente an ihren Kooperationspartner United States Postal Service (USPS). Auf der Grundlage dieser Informationen, die der Kunde zwingend bei der Zollabwicklung zur Verfügung stellen muss, werde die Verzollung der Waren im Bestimmungsland vorgenommen. Der Kunde werde darauf hingewiesen, dass die Sendung im Rahmen der zollrechtlichen Abwicklung von den Zollbehörden beschaut und geöffnet werden kann. Auch die EU habe mittlerweile Anforderungen für vorab zu übermittelnde elektronische Daten für die Verzollung beschlossen (Härpfer www.zeit.de 21.01.2008; 22.01.2008; Krempl www.heise.de 22.01.2008; vgl. DANA 3/2004, 33; Stellungnahme der Deutsche Post World Net 21.01.2008).



Bund
Personenbezogene Seeverkehrs-überwachung

Am 23.01.2008 beriet der federführende Verkehrsausschuss des deutschen Bundestags einen Gesetzentwurf der Bundesregierung zur Änderung „seerechtlicher, verkehrsrechtlicher und anderer Vorschriften mit Bezug zum Seerecht". Dabei soll eine Regelung in das Seeaufgabengesetz aufgenommen werden, wonach die zuständigen Behörden neben Identifikationsmerkmalen von Schiffen und deren Eigentümern u.a. auch persönliche Daten der an Bord befindlichen Reisenden erfassen sollen - neben Namen und Geschlecht, Geburtstag, Ausweis- und Visanummer und Staatsangehörigkeit sowie Informationen über den letzten Auslauf und den nächsten Anlaufhafen sowie weitere statistische Daten der Reise. Die Daten dürfen gemäß dem Entwurf an andere öffentliche Stellen übermittelt werden, „wenn dies zur Erfüllung von Aufgaben nach diesem Gesetz erforderlich oder durch bereichsspezifische Ermächtigungsgrundlage erlaubt ist". Die Bundespolizei erhält die Daten zur Gewährleistung des grenzpolizeilichen Schutzes des Bundesgebietes sowie zur Gefahrenabwehr. Auch eine Übermittlung ins Ausland ist vorgesehen. Es wird davon ausgegangen, dass im Jahr mindestens 16 Mio. Datensätze anfallen; sollte der gesamte Fährverkehr von der Registrierpflicht erfasst werden, könnten jährlich 29 Mio. Passagierdaten anfallen. Den deutschen Sicherheitsbehörden geht es darum, Passagiere zu erkennen, die an Bord von Schiffen gehen und dort anderes als eine Reise im Sinn haben. Eines der Szenarien für einen Terroranschlag ist, dass Terroristen ein Schiff kapern und mit Sprengstoff beladen in einen Hafen steuern. Schon bisher werden von den Reedereien Passagierlisten erstellt, allerdings v.a. für den Fall, dass ein Schiff in Seenot gerät. Dann will man wissen, wer gerettet und wer noch vermisst ist. Kritisiert wird der Vorschlag von Hans-Michael Goldmann, Sprecher der FDP-Fraktion für Häfen und Schifffahrt. Damit würden etwa Inselurlauber und selbst Tagestouristen „einfach unter Generalverdacht gestellt. Ebenso gut könnte man bei Bussen und Bahnen im Fernverkehr solche Kontrollen einführen." Auf die Reedereien kämen „unnötige Kosten und Hemmnisse" zu. Unklar sei, wie die geplante Erfassung aller Ladungen und Schiffsbewegungen in der Praxis funktionieren soll. In deutschen Häfen seien allein 2005 über 2.800 Mio. Tonnen Güter umgeschlagen worden. Anstatt die nächste „Monsterdatei" über die 29 Mio. Schifffahrtsgäste pro Jahr in Deutschland zu schaffen, solle die Bundesregierung endlich den Zoll vernünftig ausstatten (Krempl www.heise.de 22.01.2008; Ramelsberger SZ 24.01.2008).

Bund
Einheitliche Behördenrufnummer 115

Die Bundesnetzagentur plant, die dreistellige Zahlenkombination „115" als bundesweite Behördenrufnummer freizugeben. Darunter sollen Bürger-Innen künftig jederzeit eine Verwaltungsmitarbeiterln erreichen, die ihnen in Behördendingen weiterhilft und sie weitervermittelt. Vorbild ist die Nummer 311 in New York, wo 120 Behörden über diese Tastenkombination erreichbar sind. 2008 sollen zunächst 13 Mio. BürgerInnen in vier Modellregionen die Nummer anwählen können. Nach Angaben des Staatssekretärs im hessischen Innenministerium Harald Lemke werden dies Hamburg, Berlin, das Rhein-Main-Gebiet und 11 Kommunen in Nordrhein-Westfalen sein (SZ 07.12.2007, 5).

Bund

Grünen-Politiker vergleicht Schäubles Sprache mit der der RAF

In der Debatte über den Etat seines Ministeriums musste sich Bundesinnenminister Wolfgang Schäuble massive Kritik anhören. Angesichts der massiven Einschränkung der Freiheitsrechte und der Verschärfung der Sicherheitsgesetze warnte der FDP-Abgeordnete Hartfrid Wolff von „panischen Gesetzgebungsattacken". Der Grünen-Politiker Wolfgang Wieland hielt Schäuble vor, er bediene sich im Kampf gegen den Terrorismus einer Wortwahl wie die Rote Armee Fraktion (RAF). Es stimme nicht, dass „in den Metropolen Krieg herrsche". Einen „solchen Müll" habe er zuletzt von Andreas Bader gehört. Aber das sei ein Terrorist gewesen und nicht der Verfassungsminister. Während Schäuble die Unterscheidung zwischen innerer und äußerer Sicherheit, zwischen ziviler Rechtsordnung und Kriegsrecht aufheben wolle und bei der Frage der Liquidierung von Terrorverdächtigen lande, habe Bader vom Krieg in den Metropolen geredet und die RAF-Häftlinge als Kriegsgefangene bezeichnet. Er warf Schäuble vor, mit dem BKA-Gesetz, in dem die Online-Durchsuchung geregelt werden soll, eine Politik „der Zentralisierung und des Überwachungsstaates" zu betreiben. Der Etat des Bundesinnenministeriums für 2008 mit 5,07 Milliarden Euro - fast 600 Mio. Euro mehr als im Vorjahr - wurde mit den Stimmen der Koalitionsfraktionen angenommen (www.tagesschau.de 29.11.2007; SZ 30.11.2007, 5).



Bund

Regierung plant Bundesabhörzentrale

Gemäß einer Antwort auf eine parlamentarische Anfrage plant die Bundesregierung für die Ämter für Verfassungsschutz, Bundespolizei und Bundeskriminalamt sowie die Landeskriminalämter beim Bundesverwaltungsamt eines Bundesabhörzentrale einzurichten. Durch die gemeinsame Nutzung von Software und Servern sollen Kosten eingespart werden. So wird voraussichtlich eine eigentlich für das Bundesamt für Verfassungsschutz bestellte neue Abhöranlage allein 40 Millionen Euro kosten. Bislang führen die einzelnen Abhörbehörden ihre Maßnahmen in eigener Regie und mit eigener Technik durch. Die IT-Ressourcen sollen technisch so gestaltet werden, dass „diese auf Wunsch auch von anderen Bedarfsträgern genutzt werden" können. Trotz der Nutzung einer gemeinsamen Zentrale, die als reiner IT-Dienstleister fungiere, werde die Trennung von Polizei und Geheimdiensten gewahrt: „Die behördenspezifische Trennung würde für jede einzelne Maßnahmen durch technische Gegebenheiten sichergestellt. Da das eine reine IT-Dienstleistung und damit Organisationsmaßnahme sei, müsse hierüber im Bundestag nicht verhandelt werden.

Der grüne Innenexperte Wolfgang Wieland hält das Konzept dennoch für einen „weiteren Schritt zur Aufhebung der Trennung von Polizei und Nachrichtendiensten". Der FDP-Innenpolitiker Max Stadler äußerte „Unbehagen". Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Peter Schaar gab zu bedenken, dass administrative oder softwaregesteuerte Zugriffsbeschränkungen schnell aufgehoben werden könnten: „Viele Erfahrungen belegen, dass, wenn solche Möglichkeiten gegeben sind und sich eine entsprechende Änderung der politischen Großwetterlage ergibt, etwa wenn sich die Sicherheitslage zuspitzt, dass dann diese Informationen zusammengeführt werden" (www.heise.de 10.11.2007; Wallet Schleswig-Holstein Ztg. 13.11.2007, 7; Borchers www.heise.de 22.12.2007).

Bund

SPD will Grundrecht auf Informationsfreiheit im Internet

SPD-PolitikerInnen befürworten eine Verfassungsänderung, mit der ein Grundrecht auf Informationsfreiheit im Internet eingeführt würde. SPD-Innenexperte Dieter Wiefelspütz: „Das Internet ist ein neuer Raum der Freiheit, der im Grundgesetz nicht vorkommt. Die Menschen gehen dort gesellschaftlichen, kulturellen und wirtschaftlichen Betätigungen nach, sie kommunizieren und informieren sich. Es ist unsere Aufgabe, diese Ausübung von Bürgerrechten gegen staatliche Eingriffe zu schützen." Justizministerin Brigitte Zypries soll der Idee dieses neuen „Kommunikationsrechtes" aufgeschlossen gegenüberstehen. Die SPD will damit wieder ein wenig Land im Hinblick auf die Wahrung von Bürgerrechten gewinnen, nachdem sie die Vorratsdatenspeicherung und andere Erweiterungen der staatlichen Überwachung unterstützt hat. Offensichtlich plante die Justizministerin, sich anlässlich der zu erwartenden negativen Entscheidung des Bundesverfassungsgerichtes zur Online-Durchsuchung zu der Möglichkeit einer Verfassungsänderung äußern. Grundrechte wie die Un-verletzlichkeit der Wohnung und das Fernmeldegeheimnis seien, so hatten sich auch Verfassungsrichter bereits geäußert, dem Internetzeitalter nicht mehr angemessen. Nach Klaus Uwe Benneter stehen alle RechtspolitikerInnen der SPD hinter dem Vorstoß für ein neues Grundrecht. Sebastian Edathy (SPD), Vorsitzender des Innenausschusses des Bundestags, meinte, es gehe nicht nur um die Rechtmäßigkeit der Online-Durchsuchung, sondern z.B. auch um die Frage, inwieweit IP-Adressen der BesucherInnen von Webseiten der Bundesregierung gespeichert werden dürfen. Mit einem Kommunikationsgrundrecht müsse der Bürger nicht mehr fürchten, bei Einkäufen im Internet oder beim Surfen auf der Suche nach Informationen vom Staat überwacht zu werden (Telepolis www.heise.de 18.11.2007).

Bund

Alkohol-Bluttest vor dem Aus

AlkoholsünderInnen im Straßenverkehr soll nach dem Vorschlag der Innenminister von Bund und Ländern



vom 07.12.2007 künftig kein Blut zur Untersuchung des Alholgehaltes mehr abgenommen werden. Es soll reichen, wenn verdächtige Personen durch das Blasen in ein entsprechendes Röhrchen ihren Alkoholgehalt im Atem festgestellt bekommen. Derzeit wird eine Blutabnahme fällig, wenn beim Atemtest mehr als 1,1 Promille angezeigt werden. Im Jahr 2006 mussten in Deutschland mehr als 50.000 VerkehrssünderInnen zum Bluttest. Der Innenminister von Nordrhein-Westfalen Ingo Wolf (FDP) erläuterte: „Eine Blutprobe ist immer auch ein Eingriff in die körperliche Unversehrtheit, die sich angesichts des technischen Fortschritts heute vermeiden lässt". Zudem ist der Atemtest billiger und verkürzt für VerkehrssünderInnen die Wartezeit bei der Polizei (Ramelsberger SZ 08./09.12.2007, 1, 6).

Bund

Schäuble vergleicht Datenschützer mit Hitler



Bundesinnenminister Wolfgang Schäuble äußerte im Vorfeld der entscheidenden Lesung des Bundestages zur Neufassung der Telekommunikations-überwachung angesichts der massenhaft erklärten Bereitschaft, gegen die damit beschlossene Vorratsspeicherung von TK-Verbindungsdaten vor Journalisten und Richtern in Karlsruhe zu klagen: „Wir hatten den ´größten Feldherrn aller Zeiten`, den GröFaZ, und jetzt kommt die größte Verfassungsbeschwerde aller Zeiten". Nach diesem Hitler-Vergleich bezeichnete die FDP-Innenexpertin Gisela Piltz den Innenminister als „nicht mehr tragbar": „Eine Verfassungs-beschwerde, die auf die Verteidigung der Grundrechte gerichtet ist, in Beziehung zum menschenverachtenden Unrechtsregime des Dritten Reichs zu setzen, ist völlig inakzeptabel und geschmacklos". Damit habe Schäuble als Verfassungsminister „die rote Linie überschritten" (Krempl www.heise.de 20.11.2007).

Bund

DOSB plant Wettkampf-Pass als Kundenkarte

Auf der Vollversammlung des Deutschen Olympischen Sportbundes (DOSB) am 08.12.2007 in der Handelskammer Hamburg wurde unter Tagesordnungspunkt 10 das Konzept vom „Deutschen Sportausweis" vorgestellt. Gemäß DOSB-Präsidiumsbeschluss sollte der Sportausweis „zum 1. Januar 2008 endlich Wirklichkeit werden". Ziel dieser Plastikkarte ist es nicht nur, eine bundesweit einheitliche Mitgliedskarte für SportlerInnen zu schaffen. DOSB-Medienchef Gerd Graus meinte, man könne „so eine Karte sicher später mal um Vermarktungsmöglichkeiten erweitern". Betroffen sind rund 90.000 Vereine mit rund 27 Millionen Mitgliedern. Vorgestellt wurde das Projekt „Sportausweis" im Bericht des DOSB-Präsidiums unter „Konsolidierung der Finanzlage". Im Frühjahr 2007 wurde geräuschlos die „Deutsche Sportausweis GmbH (DSA)" gegründet. Deren Ziel ist ein „Drittvermarktungsmodell" mit dem „Zugriff auf größte Community". Die Karte soll erst als Mitgliedsausweis etabliert werden, um dann mit zusätzlichen Funktionen einer Kundenkarte erweitert zu werden: „Mitgliedausweis in Sportvereinen, Wettkampfpass, Beschreibung von Schnittstellen zur Integration von Mitgliederdaten in die gängige Vereinssoftware, Anschluss an Kundenbindungs- und/oder Vorteilsprogramme von Wirtschaftspartnern, optionale PrePaid-Funktion, optionale Kreditkarte als Zweitkarte". Die im DOSB organisierten Sportverbände verpflichten sich, ihren Vereinen den Einsatz des Sportausweises „dringend zu empfehlen" und „weitere Einsatzmöglichkeiten" zu prüfen.

Zuvor hatte der Deutsche Fußballbund (DFB) erfolglos ein Vorteilsprogramm für seine Mitglieder erwogen. DFB-Präsident Theo Zwanziger: „Es geht nur um die Adressen". Die DSA will nun mit den Adressen werben per „Magazin, Newsletter, Direct-Mailings und Mobiles Marketing über DSA-Datenbanksystem". Die DSA-Muttergesellschaft Athletic Sport Sponsoring (ASS) kündigt derweil über ihre Website ein „einzigartiges Zielgruppenmarketing" an. Sie könne „mit unseren Wirtschaftspartnern die rund 27 Millionen organisierten Vereinsmitglieder deutscher Sport-vereine in viele kleine, mittlere und große exklusive Zielgruppen einteilen" - z.B. nach Funktion, Region, Sportart oder Geschlecht. Die Landessportbünde, die zuvor in München über das Vorhaben informiert wurden, nahmen das Vorhaben zwar grds. zustimmend zur Kenntnis, baten aber den DOSB, auch ihre Bedenken zur Kenntnis zu nehmen. Fragen des Datenschutzes stehen im Raum, Fragen nach dem administrativen Aufwand, der durch die neue Qualität der Datenpflege entsteht, sowie steuer- und organisationsrechtliche Fragen. Thomas Kern, Pressesprecher des Bayerischen Landessportverbands: „Wir geben unsere Daten ungern an Dritte."

Gemäß Hauptgeschäftsführer Rainer Hipp vom Landessportbund Baden-Württemberg ist sein Verband „in der Überlegungsphase". Aus seinem Haus kam die Karten-Idee; 2004 startete auf Vermittlung der ASS ein Pilotprojekt mit einem großen Warenhaus mit dem Versprechen auf Rabatte für die Mitglieder, einer Einnahmequelle für den Verband und der Erleichterung bei der Mitgliederverwaltung. Das Projekt erwies sich als kompliziert, weil nach Datenschutzrecht jedes Vereinsmitglied selbst über die Funktionen seiner Karte entscheiden muss. Aus kartellrechtlichen Gründen durfte das Warenhaus auch keine außergewöhnlichen unverhältnismäßigen Rabatte gewähren. Das Projekt endete 2006. Der Landessportbund Niedersachsen war auch in das Pilotprojekt eingebunden und hat den Ausweis als „Dankeschön-Karte" an 90.000 FunktionärInnen und ÜbungsleiterInnen in den Vereinen verteilt, verbunden mit den Warenhaus-Rabatten. Dessen Direktor Reinhard Rawe, der zu den „glühenden Anhängern" der Karte gehört, sieht schon alle Datenschutzprobleme als gelöst an: Die Vereine sollen die Karten ausgeben und auch darüber entscheiden, mit welchen kommerziellen Angeboten diese geladen werden. Die Nutzung der kommerziellen Angebote liege

allein in der Entscheidung des einzelnen Mitglieds. Außerdem seien die Karten anonymisiert.

Die offiziellen Datenschutzbehörden sind mit dem Projekt noch nicht befasst worden. Weder das für den DOSB und die geplante Sportausweisverwaltungs GmbH zuständige Regierungspräsidium Darmstadt noch die für die DSA zuständige Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) wurden bisher informiert. Die Datenschützerin Renate Hillenbrand-Beck aus Darmstadt meinte, ein „so großes Projekt sollte datenschutzrechtlich sehr sorgfältig geprüft werden". Die Einwilligung von Vereinsmitgliedern müsse auf freier Entscheidung basieren und „gut informiert" sein. Eine Zwangskoppelung mit Kundenkartenanwendungen sei zu vermeiden und es dürften „keine Konsumprofile an Vereine und Sportbünde zurückfließen". Laut DSA-Geschäftsführer Stephan Penz wurde dies alles berücksichtigt.

Die Vereine wurden bisher über das Projekt noch nicht informiert. Bei Eintracht Hildesheim etwa, mit über 7500 Mitgliedern größter Verein Niedersachsens, wunderte sich Vorstandschef Rolf Altmann sehr. Sein Verein hat auch bald eine Karte, aber in Kooperation mit dem Turnerbund. Vom Sportausweis hatte er noch nichts gehört: „Das wurde unzureichend kommuniziert" (Hahn/Kistner SZ 07.12.2007, 35).

Bund

CDU fordert Offenlegung von SportlerInnen-Einkommen

Der finanzpolitische Sprecher der Unions-Bundestagsfraktion Otto Bernhardt forderte, die Einkommen nicht nur von Spitzenverdienern in der Wirtschaft, sondern auch von SportlerInnen in den Blick zu nehmen. Im Sport und in den öffentlich-rechtlichen Medienanstalten würden teils exorbitante Gehälter gezahlt. Sollte die SPD bei ihrer Forderung bleiben, die Transparenzpflicht für Manager zu verschärfen, müssten die neuen Regelungen „eins zu eins" auf andere Bereiche übertragen werden. Die hohen Gehälter von Sport- und Fernsehstars würden zu einem Teil aus den Rundfunkgebühren gespeist. Die Bundesbürger hätten somit Anspruch auf eine gewisse „Grundtransparenz": „Bei den Spitzensportlern liest man ja noch ab und zu in der Zeitung, was sie in etwa verdienen. Bei den Fernsehgrößen aber tappen wir völlig im Dunkeln" (Hulverscheidt SZ 15.01.2008, 6; s.o. S. Jungjohann, S. 22 ff.).

Bund

StudiVZ nimmt AGB-Änderung nach Protesten teilweise zurück

Die Online-Studierenden-Community „StudiVZ" hat einseitig seine Allgemeinen Geschäftsbedingungen (AGB) geändert, um in verstärktem Maße gezielte Werbung, sog. Targeting, betreiben zu können. Die Nutzenden sollten zustimmen, dass „alle möglichen Informationen" zur personalisierten Werbung verwendet werden können. Die Auswertung für Marketingzwecke sollte den sog. Clickstream, also jeden Mausclick bei der Benutzung des Dienstes und aller Inhalte, welche die Betroffenen dort einstellen, mit umfassen. In der AGB enthalten war auch die Erlaubnis zur Werbezusendung per SMS oder Instant Messaging. Wer der neuen AGB nicht bis zum 09.01.2008 zustimmte, wurde abgeschaltet. Geschäftsführer Marcus Riecke: „Werbungstreibende können in Zukunft Merkmale auswählen wie Alter, Geschlecht, Wohnort/Uni-Standort und Studienfachrichtung und ihre Werbung gemäß diesen Kriterien steuern." Das sei notwendig, um StudiVZ weiterhin als kostenloses Portal zu betreiben. Die Nutzenden wurden über die AGB-Änderung am 13.12.2007 informiert.

Ihre Reaktion kam prompt: In Foren erklärten Mitglieder massenweise ihren Austritt. Zahlreiche Mitglieder protestierten gegen die Verwendung ihrer persönlichen Daten für Werbezwecke. Sie entfernten Fotos und Informationen, anonymisierten ihre Profile, veränderten ihre Identität zu Phantasiekreationen oder bezeichneten den Betreiber in Diskussionsforen als „StasiVZ". Das Konterfei von Wolfgang Schäuble und „Stasi 2.0"-Sprüche tauchten auffällig oft auf. Die Organisation des Studi-Streiks erfolgte in 53 Gruppen mit Namen wie „Neue AGB - Ich muss mal austreten" oder „Ich bin dann mal weg". Die größte Protestgruppe „Achtung - StudiVZ ändert die AGB" hatte nach 5 Tagen mehr als 7500 Mitglieder. Ein „Arno Nym" meinte: „Was mich an dieser Angelegenheit stört ist, dass dieses Unternehmen momentan mit meinem Vertrauen spielt. Den Leuten von StudiVZ werfe ich immer noch vor, dass sie ihre soziale Verantwortung vernachlässigen." Der Druck der Community war so groß, dass das Unternehmen schon zwei Tage später zurückruderte. In einer weiteren E-Mail wurden die Mitglieder besänftigt: „Wir haben beschlossen, die SMS- und Instant-Messenger-Werbung aus den Datenschutzerklärungen herauszunehmen. Diese Form der Werbung wird es damit bei StudiVZ auch zukünftig nicht geben." Ein Verkauf von Mitgliederdaten an Dritte sei nicht beabsichtigt. In zwei weiteren Kritikpunkten hat das Unternehmen seine AGB geändert. Ursprünglich sollten Beiträge von Aussteigern aus dem Netzwerk weiterhin öffentlich zugänglich bleiben. Jetzt will StudiVZ alle persönlichen Daten nach Beendigung der Mitgliedschaft löschen. Die Frist zur Zustimmung zu den AGBs wurde verlängert: „Bis zum 31. März 2008 bleiben eure Profile für alle anderen Mitglieder sichtbar." Tatsächlich hatte 1% der StudiVZ-Mitglieder zum 11.01.2008 dem Dienst den Rücken gekehrt - immerhin 45.000 Jugendliche. 75% hatten bis zum Stichtag die AGB akzeptiert. Ob das übrig bleibende knappe Viertel bis zum 31.03.2008 zustimmte, ist nicht bekannt.

Der Bundesdatenschutzbeauftragte Peter Schaar reihte sich in den Chor der KritikerInnen ein und bezeichnete die Vermarktungspläne als unlauter und im Prinzip ungesetzlich. Kein StudiVZ-Nutzer habe bei seiner Anmeldung und Preisgabe persönlicher Daten deren kommerzieller Nutzung zugestimmt. Solche Koppelungen seien im Datenschutzrecht verboten. Am 20.12.2007 traf sich Riecke mit dem zuständigen Berliner



Datenschutzbeauftragten Alexander Dix. Riecke betonte, dass Mitglieder zielgerichtete Werbung und damit auch die Verwendung ihrer Daten über eine „Opt-out“-Funktion verhindern können, was von Dix bestätigt wurde. Eine abschließende Bewertung wollte Dix angesichts der noch laufenden Gespräche nicht abgeben.

Im deutschsprachigen Raum gibt es 2,3 Mio. Studierende. StudiVZ hat 4 Mio. Mitglieder. Trotz der enormen Reichweite schreibt die Firma angeblich Verluste, weil, so Branchengerüchte, die Netzwerke pro sichtbarem Online-Werbebanner nur 20% des üblichen Preises erzielen könne. Die Nutzenden solcher Portale seien zu aktiv. Sie klickten auf sehr viele Seiten und bekämen einen Banner gleich mehrmals zu Gesicht, was den Preis drückt. Anfang 2007 hat der Verlags-Konzern Holtzbrinck das Portal für mindestens 50 Mio. Euro gekauft. Auch das US-amerikanische Vorbild für StudiVZ, die Studierenden-Community Facebook, für deren 1,6%-Anteil Microsoft im Oktober 2007 240 Mio. Dollar zahlte, hat vergleichbare Probleme. Auch dort musste nach massiven Protesten gegen eine Werbeform, die das Nutzungsverhalten auch außerhalb der Community ausspähte, das Unternehmen seinen Mitgliedern die Möglichkeit einräumen, diese Werbung gänzlich auszuschalten (zu Facebook siehe auch unten S. 38; Hauck SZ 17.12.2007, 1; Wieschowski www.spiegel.de 18.12.2007; Krempl www.heise.de 18.12.2007; www.heise.de 21.12.2007; SH:Z 14.01.2008, Ratgeb1)

Bund

Bild verhöhnt Deutschen Presserat

Unter der Überschrift „Irre! Presserat rügt ´Bild` wegen dieses Brandstifters“ berichtete die Bild-Zeitung am 27.11.2007 auf 110 Zeilen über eine Maßregelung des Blattes durch den Presserat, die etwa zweieinhalb Monate vorher ergangen war. In seiner Ausgabe vom 19.05.2007 hatte die Zeitung unter der Schlagzeile „Warum lassen wir uns von so einem terrorisieren“ über den Deutsch-Libanesen Khaled el-Masri berichtet, der 2004 von der CIA nach Afghanistan verschleppt, monatelang festgehalten und vermutlich auch misshandelt worden ist. Die Zeitung bezeichnete den Schwaben als „Islamisten“, „durchgeknallten Schläger“, „Querulanten“, „Brandstifter“ und fragte, ob er ein Lügner sei. Nach einem Brandanschlag auf einen Metro-Markt sitze der „irre Deutsch-Libanese“, der als „angebliches Folter-Opfer die Bundesregierung, Parlament und Öffentlichkeit terrorisiert“ habe, in einer Psychoklinik und warte auf „sein Gutachten, ob er schuldfähig ist - oder einfach nur irre“. Darauf kommentierte die Frankfurter Allgemeine Sonntagszeitung: „Diese Entgleisung ist selbst für Bild-Standards beachtlich“. Auf Grund von zwei Beschwerden erkannte der Presserat in dem Bild-Bericht „eine Verletzung des Persönlichkeitsrechts“, weil der offenkundig psychisch kranke Mann als irre bezeichnet worden sei: „Diese Art der Darstellung geht gerade im Hinblick auf diese Krankheit el-Masris eindeutig zu weit“. Jetzt erklärte Bild unter Bezug auf die Rüge: „Wir stehen zu unserer Darstellung. Wir werden unsere Berichterstattung nicht weichspülen - so wenig wie bei Hasspredigern, Nazis oder sonstigem durchgeknallten Gesindel“.

Nach Ziffer 16 des Pressekodexes entspricht es „fairer Berichterstattung ... öffentlich ausgesprochene Rügen abzudrucken, insbesondere in den betroffenen Presseorganen“. Die Art des Abdrucks war dann doch für den Geschäftsführer des Deutschen Presserates als Selbstkontroll-Gremium der Printmedien, Lutz Tillmanns, verblüffend. Ob die sehr spezielle Berichterstattung von Bild über eine öffentliche Rüge der Bild erneut ein Fall für den Presserat wird, ist unklar. Der Anwalt von el-Masri, Manfred R. Gnjdic, kündigte jedenfalls eine Strafanzeige wegen übler Nachrede und Beleidigung gegen die Verantwortlichen an (Leyendecker SZ 30.11.2007, 19; zum Fall el-Masris vgl. auch DANA 3/2006, 133 f.).

Bund

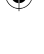
Tele2 zahlt Vertragsstrafe für illegale Telefonwerbung

Die Verbraucherzentrale (VZ) Bayern hat sich mit dem Tele-kommunikationsanbieter Tele2 aus Düsseldorf in einem außergerichtlichen Vergleich darauf geeinigt, dass das Unternehmen wegen unerlaubter Telefonwerbung ein Strafgeld in Höhe von 240.000 Euro bezahlt. Der Einigung war ein Klageverfahren am Landgericht (LG) Düsseldorf (Az. 38 O 145/06) vorausgegangen. Darin war Tele2 verurteilt worden, es künftig zu unterlassen, VerbraucherInnen ungebeten, d.h. ohne ausdrückliche Einwilligung, zu Werbezwecken anzurufen. Da es weitere Beschwerden gab, leitete die VZ ein Ordnungsgeldverfahren ein. Tele2 hätte einem Beschluss des LG zufolge 100.000 Euro an den Staat zahlen müssen. Dagegen legte das Unternehmen Beschwerde ein. Auf Grund neuer Fälle startete die VZ ein zweites Verfahren, in dem Tele2 eine weitere Strafe in ähnlicher Höhe drohte. Angesichts dieser Entwicklung einigte sich der Anbieter mit den Verbraucherschützern dann außergerichtlich und verpflichtete sich gegen Rücknahme der Vollstreckungsanträge, eine Vertragsstrafe an die VZ zu zahlen. Allerdings betrifft diese Zahlung nur unerlaubte Werbeanrufe in der Vergangenheit. Da das Urteil nach wie vor Rechtskraft hat, können künftige Verstöße wiederum von der VZ verfolgt und geahndet werden. Marion Breithaupt-Endres, Vorstand der VZ Bayern: „Eine derart hohe Konventionalstrafe hat für Verbraucherorganisationen einen absoluten Seltenheitswert“. Tele2 betonte, die Firma habe sich stets für ein sauberes Telefonmarketing nach den Grundsätzen der deutschen Rechtsprechung eingesetzt. Man arbeite nur mit renommierten Adresslieferanten zusammen, die Tele2 vertraglich garantierten, dass für jede Adresse eine gültige Einwilligungserklärung vorliege (Kieler Nachrichten 24.11.2007, 6; SZ 24./25.11.2007, 28).

Bund
Zirkuszentralregister

Der Bundesrat stimmte am 30.11.2007 für das Gesetz zur Einführung eines Zirkuszentralregisters. Dieses soll den Behörden länderübergreifend Informationen zu jedem Zirkus verschaffen. Bisher war Ämtern in vielen Fällen nicht bekannt, ob z.B. eine Erlaubnis für den Betrieb eines Zirkus‘ in einem anderen Bundesland erteilt worden war. Mit dem Register, in dem alle verfügbaren Daten gespeichert werden, soll die Kontrolle vereinfacht und damit auch der Tierschutz verbessert werden. Es wird eine Verordnung zum Register geben. TierschützerInnen geht die Neuregelung allerdings noch nicht weit genug. Sie fordern ein Haltungsverbot für bestimmte Wildtiere im Zirkus, z.B. auch für Elefanten (SZ 01./02.12.2007, 2).

Bund
German Privacy Foundation gegründet



Der neu gegründete, gemeinnützige Verein „German Privacy Foundation“ hat sich zur Aufgabe gemacht, das Fachwissen und den Berufsschutz von JournalistInnen, JuristInnen und IT-Fachleuten zu bündeln, um in Zeiten der Vorratsdatenspeicherung über anonyme und verschlüsselte Kommuni kationsmöglichkeiten zu informieren und auch selbst technische Lösungen anzubieten. Vom Verein angebotene Schulungen sollen dazu beitragen, dass über die Sicherheit im Internet in den Medien „besser und sachgerechter“ berichtet wird. Weil es in Deutschland auf Grund der zunehmenden Verwendung von IP-Adressen in Strafverfahren immer häufiger zu Ermittlungen gegen die Betreiber von TOR-Nodes des Anonymisierungsdienstes kommt, will die German Privacy Foundation sowohl TOR-Admins als auch Polizeibehörden und Staatsanwaltschaften unterstützen, um die Zahl der TOR-Raids zu verringern. Dem dient die technische Aufklärung der Ermittler wie auch ein Log-Service für das TOR-Netz. Damit könne man „im Falle von Ermittlungen gegen TOR-Admins den Nachweis erbringen ..., dass der TOR-Node zum Tatzeitpunkt online war und ein Missbrauch des Dienstes möglich ist“. In Ausnahmefällen will die German Privacy Foundation privaten Betreibern von Anonymisierungsdiensten auch Rechtsbeistand vermitteln. Zur Kontaktaufnahme bietet der Verein eine „vorratsdatenfreie Nachrichtenbox“, bei der die Nachrichten auf dem Server gespeichert werden. Weil dabei auch nach den neuen Regeln zur Vorratsdatenspeicherung keine rechtliche Verpflichtung zum Festhalten der Absender- und Empfängerdaten besteht, kann auf diese Weise anonym kommuniziert werden (Telepolis www.heise.de 06.12.2007).

Bund
Alle Sexualdelikte ins Führungszeugnis?

Über eine Bundesratsinitiative „zur Änderung des Bundeszentral-registergesetzes“ strebt die bayerische Justizministerin Beate Merk an, jede Verurteilung wegen Kinderpornografie, jede Verletzung der Fürsorge- und Erziehungspflicht und jede Misshandlung von Schutzbefohlenen in das polizeiliche Führungszeugnis aufzunehmen. Ziel ist es zu verhindern, dass private Kindergärten und Schulen versehentlich verurteilte Sexualstraftäter als Lehrkräfte oder ErzieherInnen einstellen: „Die Einrichtungen müssen solche Verurteilungen kennen, alles andere ist unverantwortlich gegenüber den Kindern.“ Bislang erfolgt eine Eintragung nur bei Verurteilungen zu einer Geldstrafe von mehr als 90 Tagessätzen oder Freiheitsstrafen von mehr als drei Monaten bei Erwachsenen. Bei Jugendlichen muss die Strafe sogar mehr als zwei Jahre betragen, es sei denn, die wurde nicht zur Bewährung ausgesetzt (Der Spiegel 4/2008, 18; SZ 21.01.2008, 2).

Bayern
Auskunftsverweigerung zu Überwachungsmaßnahmen

Die bayerische Staatsregierung und die regierende CSU verweigerten im Landtag die Auskunft über Lauschangriffe und Online-Durchsuchungen im Freistaat. Die CSU lehnte am 23.01.2008 einen Antrag der Grünen ab, wonach die Staatsregierung einen Bericht über die Spähmaßnahmen geben sollte. Als Grund wurde die Sicherung der Vertraulichkeit genannt. Die Informationen würden nur dem Parlamentarischen Kontrollgremium oder einem anderen geheim tagenden Organ vorgelegt. Normalerweise stimmt die CSU Berichtsanträgen zu. Anders jetzt beim Thema Lauschangriffe. Die Grünen wollten wissen, aus welchen Gründen wieviele BürgerInnen in Bayern seit 2003 abgehört werden, welche Techniken bei Lauschangriffen auf die Wohnung und die Telekommunikation eingesetzt werden. Die Grünen und die SPD kritisierten die Verweigerung, so etwa der Münchner SPD-Abgeordnete Florian Ritter: „Es gibt überhaupt keinen Grund, warum die Staatsregierung nicht berichtet.“ Die CSU argumentierte, die Politik dürfe die technische Entwicklung nicht ignorieren, so etwa der CSU-Abgeordnete Herbert Ettengruber: „Wenn Verbrechensabredungen im Internet getroffen werden, muss die Politik darauf reagieren“ (www.heise.de 23.01.2008).

Bayern
GPS-Überwachung von Sexualstraftätern

Die Bayerische Justizministerin Beate Merk (CSU) möchte als erstes Bundesland in Deutschland nach US-Vorbild entlassene Sexualstraftäter mit einer GPS-gestützten elektronischen Fessel überwachen lassen. Damit sollen rückfallgefährdete Sexualstraftäter daran gehindert werden, bestimmte Sicherheitszonen, z.B. um Kindergärten oder Schulen, zu betreten. Merk: „Ziel ist nicht die Totalüberwachung“. Ulrich Staudigl aus ihrem Ministerium betonte,

dass es nicht darum gehe, „wie man das technisch überwachbar macht. Wir müssen prüfen, ob man mit diesem Vorschlag nicht zu weit in das Persönlichkeitsrecht eingreift von Jemandem, der seine Strafe bereits voll verbüßt hat.“ Man wolle niemanden auf Schritt und Tritt beobachten. Fernhaltebestimmungen sieht das Gesetz bereits heute vor, etwa als Auflagen im Rahmen der Führungsaufsicht. Welche Technik verwendet werden soll, ist noch nicht geklärt. Mit der GPS-Überwachung wäre der jeweilige Aufenthaltsort einer Person feststellbar. Wenn diese sich einer Sicherheitszone nähert, so könnte über eine SMS Alarm ausgelöst werden. Die Anregung für die Initiative kam wohl von der Dauerobservation eines nach 22 Jahren entlassenen Sexualmörders in Sachsen-Anhalt durch 32 PolizistInnen je Observationstag im Jahr 2007.

Bundesjustizministerin Brigitte Zypries kritisierte das Vorhaben, das rechtlich nur bei vorzeitig Entlassenen als Bewährungsauflage denkbar sei. Zur Gefahrenabwehr müsse man zu anderen Maßnahmen greifen: „Das Ganze klingt so, als sei es mit einem Verständnis von Menschenwürde nicht vereinbar.“ Die britische Regierung hatte 2007 ein Projekt mit GPS-Überwachung von Straftätern auf Grund zahlreicher Mängel abgebrochen. Die Straftäter konnten in der Nähe von großen Gebäuden nicht mehr verfolgt werden; die Kontrolle war lükkenhaft und manche der Überwachten entfernten einfach die Fußfessel oder nahmen den GPS-Empfänger nicht mit. Derzeit überlegt die britische Regierung stattdessen RFID-Chips zu verwenden (s.u. S. 41; Telepolis www.heise.de 26.01.2008; Der Spiegel 5/2008, 17; Ramelsberger SZ 28.01.2008, 5; www.justiz.bayern.de PE Merk weist Einwände zurück).



Bayern
Kirchen sollen über Vorstrafen von Religionslehrern informieren

Zum Schutz bayerischer Schulkinder vor sexuellem Missbrauch durch Religionslehrer sollen die Kirchen den Freistaat über Vorstrafen ihrer Pfarrer informieren. Hierfür setzten sich am 29.11.2007 alle drei Fraktionen im Landtag ein. Bisher war von den als Religionslehrern eingesetzten Pfarrern weder ein polizeiliches Führungszeugnis noch eine entsprechende Erklärung gefordert worden. CSU, SPD und Grüne plädierten dafür, hierzu eine Vereinbarung mit den Kirchen abzuschließen. Anlass war ein Missbrauchsfall in Riekofen, wo ein als Religionslehrer tätiger vorbestrafter Pfarrer einen Jungen missbraucht hatte. Das Bistum Regensburg hatte die Schulbehörden nicht über die Vorstrafe informiert (SZ 30.11.2007, 37)

Berlin
Knappe Mehrheit für Polizeirechts-verschärfung

Die rot-rote Koalition im Berliner Abgeordnetenhaus hat am 22.11.2007 eine heftig umstrittene Novelle des Landespolizeigesetzes mit 74 Stimmen gegen 73 Stimmen bei 2 Enthaltungen von Linkenabgeordneten verabschiedet, bei der es u.a. um die Ausdehnungen der Möglichkeiten der Videoüberwachung und der Handy-Ortung geht. Die rot-rote Koalition verfügt über insgesamt 76 Stimmen. Die drei Oppositionsfraktionen von CDU, FDP und Grünen lehnten das Gesetz ab. Kurz vor Verabschiedung der Novelle des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) hatte sich noch der Berliner Anwaltverein gemeldet und die Verfassungsmäßigkeit des Entwurfes bezweifelt, welcher der Polizei einen weit reichenden Zugriff auf Videobilder der Berliner Verkehrsbetriebe (BVG) und anderer privater Stellen erlaubt. Zudem sollten Beamte zur Eigensicherung bei der Durchführung von Verkehrskontrollen aus ihren Fahrzeugen heraus Videoaufnahmen erstellen dürfen, wobei auch unbeteiligte Dritte zwangsläufig erfasst würden. Diese Regelung wurde vom Parlamentsplenum in letzter Minute gestrichen. Kritisiert wurde auch die massive Ausweitung der Videoüberwachung bei Großveranstaltungen ohne Anhaltspunkte für das Begehen von Straftaten.

Die Humanistische Union (HU) hatte dafür appelliert, die Ausweitung der Videoüberwachung nicht abzusegnen. Gemäß einer Studie über das Pilotprojekt zur 24-Stunden-Videoaufzeichnung in Berlin hat sich diese Praxis nicht bewährt. Die von der SPD erhoffte „generalpräventive Wirkung“ sei nicht eingetreten, die Zahl der Sachbeschädigungen durch Graffiti und Vandalismus sei im Untersuchungszeitraum sogar leicht angestiegen. Die Behauptung des Entwurfes, die Videoüberwachung habe sich „als geeignetes Mittel“ zur Bekämpfung der Drogenkriminalität erwiesen, sei „völlig aus der Luft gegriffen“ (vgl. DANA 4/2007, 191).

Innensenator Ehrhart Körting (SPD) hatte sich zwei Tage vor der Verabschiedung noch auf Korrekturen eingelassen. So dürfen nun Daten von Handy-Ortungen nur mit Zustimmung der betroffenen Personen an Dritte weitergegeben werden. Der Innenausschuss nahm eine Klausel zur Evaluation der Regelungen nach zwei Jahren in das Gesetz auf. Gegen den Entwurf stimmte auch die Linken-Abgeordnetinnen Evrim Baba und Mari Weiß. Die Innenexpertin der Linken Marion Seelig räumte ein, dass es bei dem neuen Gesetz um einen „Grundrechtseingriff geht, der nicht gering ist“. Das sähen viele Mitglieder ihrer Fraktion mit sehr gemischten Gefühlen. Man habe sich aber in der Koalition nicht ganz durchsetzen können. Grünen-Fraktionschef Volker Ratzmann warf dem Senat und den Regierungsfraktionen eine Abkehr von den Freiheitsrechten vor. Rot-Rot habe mit der Novelle „die Tür ein Stück“ aufgemacht in „Schäubles Welt“. Aus Protest entrollten die Grünen-Abgeordneten bei Abgabe des Abstimmungsergebnisses DIN-A-3-große Plakate, auf denen Videokameras abgebildet waren. Mit den in Fernrohre verwandelten Blättern „filmten“ sie anschließend die Abgeordneten von Rot-Rot. Der CDU-Innenpolitiker Frank Henkel lobte den Ansatz des Vorhabens. Damit sei Rot-Rot endlich Forderungen der CDU gefolgt. Doch gehe die Ausdehnung der Überwachungsbefugnisse nicht weit genug. Es käme z.B. nicht zur Montage von Kameras an Kriminalitätsschwerpunkte

n und zur Aufzeichnung von Graffiti-Schmierereien: „Wir werden trotz aller Verbesserungen diesen halbherzigen Entwurf nicht mittragen“. FDP-Sprecher Björn Jotzo hielt Rot-Rot dagegen vor, „ein Sicherheits-Placebo auf Kosten der Bürgerrechte“ statuiert zu haben (Krempl www.heise.de 22.11.2007; Krempl www.heise.de 16.11.2007).

Brandenburg

Neues Datenschutzgesetz verabschiedet

Der Landtag in Potsdam hat am 15.11.2007 nach umfassenden Korrekturen durch den Innenausschuss den Regierungsentwurf zur Novellierung des brandenburgischen Landesdatenschutzgesetzes (LDSG) mit den Stimmen der schwarz-roten Koalition verabschiedet. Die Reform soll nach dem Willen von Innenstaatssekretär Hans-Jürgen Hohnen (CDU) der besseren Übersichtlichkeit des Datenschutzes dienen: „Dazu sind insgesamt mehr als 15 entbehrliche Normen und Standards konsequent reduziert oder gänzlich abgebaut worden“. Die brandenburgische Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht (LDA) Dagmar Hartge zeigte sich mit den Änderungen zufrieden. Anders als zunächst geplant, reduziere das verabschiedete Gesetz nicht mehr die Anforderungen an die Sicherheit der Informationsverarbeitung. Die Verpflichtung für die Verwaltung werde fortgeschrieben, in einem schriftlichen Sicherheitskonzept Maßnahmen zur Beherrschung der in der ebenfalls vorgeschriebenen Risikoanalyse festgelegten Gefahren aus dem IT-Bereich für die Grundrechte der Menschen niederzulegen und Gegenmaßnahmen zu treffen. Ebenfalls beibehalten wurde die zunächst zur Streichung vorgesehene Regelung zum Datenschutzaudit. Die entsprechende Norm war 1998 vor dem Hintergrund der rasanten Entwicklung in der Informationstechnik (IT) in das LDSG aufgenommen, aber auf Grund des fehlenden Ausführungsgesetzes nie angewandt worden. Hartge appellierte an den Gesetzgeber, hier nun bald tätig zu werden. Auch in Brandenburg müssten die öffentlichen Stellen ihre Datenverarbeitung in Punkto Datensicherheit und Datensparsamkeit durch unabhängige Gutachter zertifizieren lassen können. Sie bestätigte, dass das Gesetz anwenderfreundlicher geworden ist.



Hartge bedauerte, dass sich der Gesetzgeber nicht zur „längst überfälligen Zusammenführung der Aufsichtsbehörden für die Daten-verarbeitung des öffentlichen und des privaten Bereichs“ durchringen konnte. Dadurch hätte tatsächlich Bürokratie abgebaut und ein einheitlicher Ansprechpartner in Datenschutzfragen geschaffen werden können. Ähnlich äußerte sich der Innenexperte der Linksfraktion Hans-Jürgen Scharfenberg, der dem Innenministerium vorwarf, in dieser Frage seinen „Blockadekurs“ fortzusetzen und an seiner „antiquierten Position“ festzuhalten. Hohnen vertröstete die KritikerInnen dagegen auf das noch ausstehende Ergebnis eines entsprechenden Klageverfahrens vor dem Europäischen Gerichtshof. Der Landtag werde dazu - wie vom Innenausschuss empfohlen - bis Mitte 2008 einen Prüfbericht bekommen: „Dann haben wir alles Notwendige auf dem Tisch, um die Frage der Zusammenlegung offen zu diskutieren.“

Das Gesetz sieht auch die Einrichtung einer landeseigenen und -einheitlichen Schülernummer vor, „um individuelle schulische Bildungsverläufe von Schülern ohne namentlichen Bezug nachzuvollziehen und auszuwerten“. Ziel sei es, „im Rahmen der Aufgaben der Schulaufsicht und Schulverwaltung sichere Aussagen zur Wirksamkeit bildungspolitischer, bildungsrechtlicher und administrativer Maßnahmen für Zwecke der Planung und Steuerung sowie des optimierten Ressourceneinsatzes für das Schulsystem zu erhalten“. Die Einrichtung der automatisierten zentralen Schülerdatei soll auch „der Kontrolle und damit der Sicherung der Schulpflicht“ dienen. Ein Antrag der oppositionellen Linken zur Streichung der entsprechenden Passage erhielt keine Mehrheit (Krempl www.heise.de 15.11.2007; vgl. DANA 3/2007, 134).

Hamburg

Wohnung von G-8-Gegner verwanzt und abgehört

Die Wohnung eines 51jährigen Pflegedienstleiters in Sankt Pauli, der in einem Kirchenkreis und seit 30 Jahren in der Anti-AKW-Bewegung aktiv ist, wurde nach den Brand- und Farbbeutelanschlägen vor dem G-8-Gipfel ins Fadenkreuz des Bundeskriminalamtes genommen und - ohne jedes Ergebnis - umfassend ausspioniert mit Videoüberwachung im Hauseingang, Telefon- bzw. Internetüberwachung sowie Wanzen in allen Zimmern. Der Betroffene wurde hierüber durch ein Schreiben der Bundesanwaltschaft informiert, die gesetzlich verpflichtet ist, die Abgehörten im Nachhinein zu benachrichtigen. Die Wanzen wurden offenbar im Rahmen einer Wohnungsdurchsuchung installiert. Vom 09.05. bis 14.06.2007 belauschten die Ermittler jedes Wort in der Wohnung. Um die Wanze wieder auszubauen, müssen sich die Ermittler später heimlich Zugang verschafft haben. Hintergrund des großen Lauschangriffs waren keine eindeutigen Sachbeweise, sondern Mutmaßungen von Profilern beim Vergleich der Bekennerschreiben der Farbbeutelanschläge mit Texten aus der linken Szene. Ein Weggefährte des Wohnungsinhabers - beide Mitglieder einer Anti-AKW-Gruppe, die sich in der Roten Flora trifft und die Proteste zu Heiligendamm organisierte - passte ins Profil der mutmaßlichen Anstifter: ältere Linke. Dies genügte dem BGH-Ermittlungsrichter offensichtlich, um grünes Licht für den Lauschangriff wegen Bildung einer terroristischen Vereinigung nach § 129a StGB zu geben. Auch im Pflegedienst des Betroffenen gab es eine Hausdurchsuchung und alle Telefone wurden dort abgehört. Der Betroffene Norbert T.: „Es war ein erheblicher Eingriff. Mich hat es nicht überrascht. Doch für meine Freundin war es ein Schock, dass alle Gespräche mitgehört wurden.“ Durch das Abhören der Telefonate seiner Firma „wurden auch 50 Kollegen hineingezogen“. Auf Beschwerde beim Bundesgerichtshof (BGH) wurde



schließlich festgestellt, dass die Aktion unzulässig war. Brandanschläge gegen Sachen und Farbsprühereien genügten nicht zur Annahme einer terroristischen Vereinigung. Der Betroffene hat die begründete Befürchtung, dass die Telefonüberwachung gegen ihn weiterhin vorgesetzt wurde (www.taz.de 16.11.2007; Schäfer www.mopo.de 26.11.2007).

Hamburg

Polizei gibt beschlagnahmte Rechner an Musikindustrie-Anwalt weiter

Die illegale Praxis von Polizeibehörden, bei Hausdurchsuchungen sichergestellte Rechner an die Firma proMedia GmbH weiterzugeben, scheint sehr weit verbreitet zu sein. Die hamburger Firma des Anwaltes Clemens Rasch arbeitet als „Piratenjäger" für die Musikindustrie und geht dabei zivilrechtlich gegen Personen vor, denen der nicht lizensierte Upload von Musikdateien in Filesharing-Netzwerken vorgeworfen wird. Bei pro-Media werden nach eigenen Angaben die Festplatten gespiegelt und diese Kopien umfassend ausgewertet, wobei nicht nur auf auf Urheberrechtsverstöße basierende Dateien zugegriffen wird, sondern auf sämtliche Daten, etwa auch auf die E-Mail-Kommunikation des Computereigentümers. ProMedias Ziel ist es, durch möglichst viele Klagen und Verurteilungen eine abschreckende Wirkung zu erreichen. Zudem verdient Rasch gut durch die Gebühren für die nach Einleitung eines Ermittlungsverfahrens von ihm standardmäßig versandten Abmahnungen.



Rasch beklagte anlässlich einer Info rmationsveranstaltung am 13.11.2007, dass die Verkürzung der Speicherung der Verbindungsdaten auf 7 Tage nach dem sog. Voss-Urteil gegen T-Online (vgl. DANA 1/2006, 42, 4/2006, 191 f.) dazu führte, dass mittler-weile für etwa die Hälfte der von seiner Firma ermittelten IP-Adressen keine Nutzerdaten mehr ermittelt werden können. Solange die meisten Provider noch 80 Tage lang speicherten, habe es lediglich einen „Datenschwund" von 10 bis 15 % gegeben. Rasch betonte, dass seine Kanzlei außerhalb von vor dem offiziellen Erscheinungstermin angebotenen Musikstücken nur bei Uploads ab einer bestimmten Anzahl tätig werde, die er jedoch geheim halten wolle. Gemäß der Angabe der Anwaltskanzlei Wilde&Berger liegt diese Grenze bei 499 Stück (www.heise.de 14.11.2007).

Hessen

CDU nutzte Schulamtsdaten für Wahlwerbung

Nach einem Bericht der Frankfurter Rundschau hat die CDU Hessen einen offenen Brief an Eltern, Lehrkräfte und SchülerInnen über einen internen Verteiler der staatlichen Schulämter verschickt. In dem Schreiben vom 14.01.2008 wirbt die CDU im Hinblick auf die Landtagswahl am 27.01. für ihre Schulpolitik. Der Brief wurde laut CDU an alle Eltern- und Schulelternbeiräte, Lehrkräfte, Personalräte an Schulen, Schulleitungen, SchülerInnen und Schülervertretungen verschickt. Die Zeitung gibt an, dass die Adresszeile der E-Mail eine interne, nicht öffentlich zugängliche Kennung enthielt. CDU-Generalsekretär Michael Boddenberg meinte dagegen, der Bericht sei „schlicht falsch": „Die von uns verwendeten Daten sind allesamt im Internet frei zugänglich. Das ist der erneute Versuch einer Diffamierungskampagne." Der bildungspolitische Sprecher der Grünen Mathias Wegner sprach von einem „handfesten Skandal". Aus der E-Mail, die den Grünen vorliege, gehe eindeutig hervor, dass sie an interne E-Mail-Adressen versandt wurde: „Diese Verteiler dürfte Herr Boddenberg gar nicht kennen und schon gar nicht für Wahlwerbung benutzen" (www.heise.de 19.01.2008).

Niedersachsen

Land Schlusslicht beim Datenschutz

Nach Einschätzung des Landes-beauftragten für den Datenschutz des Landes Niedersachsen (LfD) Joachim Wahlbrink fährt sein Bundesland beim Datenschutz „im letzten Wagen". Anlässlich der Vorstellung seines Tätigkeitsberichtes kritisierte er dessen starke Vernachlässigung durch die schwarz-gelbe Regierung. Wahlbrink kritisierte vor allem seinen Dienstherrn, Innenminister Uwe Schünemann, der in Braunschweig Kameras zur Videoüberwachung „mit Bratwurst und Blasmusik" eingeweiht hat. Das Mitte November 2007 verabschiedete neue Polizeigesetz hält Wahlbrink weiterhin für verfassungswidrig. Das Bundesverfassungsgericht (BVerfG) hatte gut zwei Jahre zuvor das alte Gesetz gekippt. Obwohl das BVerfG dies ausdrücklich verboten hatte, erlaubt das neue Gesetz bei der präventiven Telekommunikationsüberwachung den Eingriff in den Kernbereich persönlicher Lebensgestaltung „im Zweifel doch". Die Einwände hätten den Landtag „nicht beeindruckt". Hans-Christian Biallas von der CDU hält die Einwände Wahlbrinks für „unbegründet". Der Eingriff in den Kernbereich sei vergleichbar mit der von CDU und SPD im Bund beschlossenen Regelung der Strafprozessordnung (Schöneberg taz 28.11.2007).

Schleswig-Holstein

Polizei hört Journalistentelefonate mit G-8-Gegnern ab

Das Landeskriminalamt (LKA) Schleswig-Holstein hat bei Ermittlungen gegen mutmaßliche Linksextremisten Telefongespräche von Redakteuren von „NDR Info", tagesschau.de, Spiegel-Online, Tagesspiegel und der „tageszeitung" im Auftrag der Bundesanwaltschaft in Karlsruhe abgehört. Entsprechende Protokolle von Gesprächen mit Informanten in Norddeutschland sind aus Ermittlungsakten bekannt geworden. Hintergrund waren offensichtlich

Ermittlungen gegen neun Personen wegen der Zugehörigkeit zu einer terroristischen Vereinigung (§ 129a StGB). Sie wurden verdächtigt, zwischen 2002 und 2006 drei Brandanschläge auf Rüstungsfirmen und einen Bundeswehrbus in Schleswig-Holstein verübt zu haben. Die Ermittlungen gegen die Antifa-Szene erfolgten zeitlich zudem im Vorfeld des G-8-Gipfels von Heiligendamm. Abgehört wurden nicht die eigenen Anschlüsse der Journalisten; vielmehr riefen diese Personen an, gegen die Ermittlungen liefen und die daher abgehört wurden. Die Verlagshäuser und die betroffenen Sender wurden nicht informiert. Die Ermittlungsbehörden gaben die Abschriften der Telefonate mit vollständiger Namensnennung der Reporter an die Anwälte der Beschuldigten weiter. Aus den Protokollen ergeben sich u.a. Redaktionsinterna und Hinweise auf redaktionelle Entscheidungsprozesse. „Dies ist ein massiver Angriff auf die Rundfunk- und Pressefreiheit", meinte NDR-Indendant Jobst Plog. „Wenn Recherchen unter Aufsicht des Staates stattfinden, dann hat das mit der Freiheit der Berichterstattung nichts mehr zu tun, sondern beeinträchtigt die Arbeitsmöglichkeiten unserer Journalisten". Für Hendrik Zörner, Pressesprecher des Deutschen Journalistenverbandes (DJV) ist der Vorgang „absolut inakzeptabel". Die Bundesanwaltschaft will die Vorwürfe prüfen, so ein Sprecher: „Da steckt aber sicher kein böser Wille dahinter."



In die Abhöraktion gerieten nicht nur Journalisten, sondern auch Rechtsanwälte. In mindestens einem Fall war ein Anwalt betroffen, dem ein Mandat erteilt worden war. Die Vorsitzende des Republikanischen Anwaltsvereins Britta Eder bewertete die Abhörmaßnahmen als rechtswidrig. Sie beantragte bei den Ermittlungsrichtern des Bundesgerichtshofes, die aufgezeichneten Telefonate zu löschen und die Protokolle zu vernichten. Der Präsident der Bundesrechtsanwaltskammer Axel Filges bekräftigte die Unzulässigkeit des Abhörens von Gesprächen zwischen Anwalt und Mandanten. Er befürchtet eine „Zwei-Klassengesellschaft", in der auf der einen Seite die „normalen" Anwälte stünden, deren Gespräche abgehört werden dürften, und auf der anderen Seite die Strafverteidiger, bei denen dies verboten ist. Die Grenze sei fließend, eine derartige Unterscheidung sei nicht praktikabel (KN 10.11.2007, 15; tagesschau.

Schleswig-Holstein

Polizei scannt Fingerabdrücke

Bei den Kriminalpolizeidienststellen in Kiel, Lübeck, Pinneberg und Rendsburg wird bei der Abnahme von Finger- und Handflächenabdrücken nicht mehr mit Papier und schwarzer Farbe gearbeitet; diese werden vielmehr mit einem Livescan-Gerät digital aufgenommen. Anschließend werden die Daten automatisch im Auskunftssystem der Polizei wie auch in der Fingerabdruck-Datenbank des Bundeskriminalamtes (BKA) gespeichert. Damit liegen alle grundlegenden polizeilichen Erkenntnisse zu einer gesuchten Person (inklusive Personenbeschreibung und Lichtbilder) in einem einheitlichen Informationssystem bereit. Der bis dahin vorgenommene zeitaufwändige Versand von Papierunterlagen entfällt. Kai Schlotfeldt vom Landeskriminalamt: „Die Möglichkeit zur Identifizierung über ihre Finger- und Hand-flächenabdrücke beschleunigt sich durch diese technische Neuerungen enorm" (Schleswig-Holstein Ztg. 21.12.2007, 3).

Umfrage

Mehr Online-Transaktionen trotz Datenschutzbedenken

Mehr als jeder Zweite (54%) vermutet nach einer Umfrage des Instituts für Demoskopie Allenbach, dass seine Daten im Netz ungeschützt sind. Mit 48% stehen staatliche Überwachungsmaßnahmen oben auf der Liste der Nutzerängste. Befragt wurden 10.369 Internetnutzende zwischen 14 und 64 Jahren. Gerade mal 11% der Befragten halten die Weitergabe persönlicher Daten im Internet für unbedenklich; 50% befürchten deren Missbrauch. 61% rechnen damit, dass Unternehmen die Benutzerdaten zu Werbezwecken nutzen, was 43% dazu veranlasst, persönliche Daten nur vertrauenswürdigen Unternehmen zu überlassen. Knapp jeder Dritte hat aus Datenschutzgründen schon häufiger darauf verzichtet, im Internet etwas zu bestellen. Trotz aller Ängste und Befürchtungen erfreut sich die Nutzung von Bankdiensten und Webshops zunehmender Beliebtheit. Waren 2006 noch 54% der Befragten Online-Kaufende, so waren es 2007 59%. Beim Online-Banking stieg die Quote von 32% auf 34% (www.heise.de 07.11.2007).



Internationale Datenschutznachrichten

Interpol

Globale Öffentlichkeitsfahndung gegen Kinderschänder

Auf der Suche nach Kinderschändern will die internationale Polizei-organisation Interpol verstärkt auf die weltweite Öffentlichkeit setzen. Interpol-Präsident Jackie Selebi teilte mit, dass auf der Jahresversammlung der 144 Mitgliedstaaten in Marrakesch am 05.11.2007 diese Maßnahme mit 115 Stimmen beschlossen wurde. Präzedenzfall war die Festnahme eines Kanadiers in Thailand im Oktober 2007, dessen Fotos weltweit per Internet verbreitet worden waren. Die Bilder hatte der Mann selbst ins Web gestellt; Experten des deutschen Bundeskriminalamtes konnten jedoch sein Gesicht entzerren. Selebi gab bekannt, dass das Einschalten der Öffentlichkeit von der Versammlung ohne Gegenstimme verabschiedet wurde (SZ 07.11.2007, 12).



Vereinte Nationen/Europa

Kritik an Terrorliste nimmt weiter zu

Die ParlamentarierInnen beim Europarat in Straßburg haben scharfe Kritik an den Terrorlisten der Vereinten Nationen (UN) und der Europäischen Union (EU) geübt. In einer mit großer Mehrheit angenommenen Resolution forderten die Abgeordneten aus 47 Staaten die europäischen Regierungen auf, die Menschenrechte zu achten. Bisher müssen auch Unschuldige nach Aufnahme in die Liste hinnehmen, dass ihre Konten gesperrt werden, ohne sich wehren zu können. Der Initiator der Resolution, der schweizer Abgeordnete und Sonderermittler des Europarats, Dick Marty, forderte die nationalen Parlamente auf, Druck für eine Reform zu machen. Für eine Privatperson, die nur auf Grund „vager Verdachtsmomente“ in das Visier des US-Geheimdienstes CIA geraten sei, bedeute ein Eintrag auf der Liste eine „zivile Todesstrafe“. Er sei enttäuscht von der „totalen Passivität der Regierungen“. Diese zeigten kein Interesse, den Kampf gegen den Terror mit rechtsstaatlichen Mitteln zu führen.

Kurz zuvor äußerte der Generalantwalt des Europäischen Gerichtshofes (EuGH) in Luxemburg Poiares Maduro die Ansicht, dass die EU-Gerichte überprüfen müssen, ob die Liste der EU mit rechtsstaatlichen Grundsätzen der EU vereinbar ist. Maduro forderte den EuGH am 16.01.2008 auf, der Klage eines saudi-arabischen Staatsbürgers stattzugeben, der von den Vereinten Nationen unter Terrorverdacht gestellt worden war und dessen Konten auch von der EU gesperrt wurden. Der Generalanwalt sieht mehrere Grundrechte des Klägers verletzt, u.a. das Eigentumsrecht und den Anspruch auf rechtliches Gehör und auf Rechtsschutz. Das EU-Gericht erster Instanz hatte die Klage des Geschäftsmannes 2005 noch abgewiesen und gemeint, die EU sei verpflichtet, die Resolutionen des UN-Sicherheitsrates zu befolgen (vgl. DANA 4/2007, 207, 1/2007, 37; 2/2006, 85 f.). Maduro plädierte jetzt dafür, dass auch völkerrechtliche Maßnahmen gegen den Terrorismus sich an rechtsstaatliche Grundsätze halten müssen.

In einem Interview mit dem „Spiegel“ äußerte sich der Präsident des deutschen Bundesverfassungsgerichtes Hans-Jürgen Papier zu dem Thema: „Es gibt Schutzpflichten des Staates seinen Bürgern gegenüber. Bei der Erfüllung dieser Pflichten dürfen aber die Freiheitsrechte der Bürger nicht unverhältnismäßig beeinträchtigt werden. Angesichts der modernen, globalen Bedrohungen, aber auch auf Grund der neuen Technologien, über die Rechtsbrecher verfügen, mag es notwendig sein, Ermittlungsbefugnisse weiter auszudehnen. Dies kann aber nur geschehen, wenn ein angemessener Ausgleich mit den Freiheitsrechten der Bürger hergestellt wird. ... Auf der Ebene des Völkerrechts ist es noch nicht gelungen, die beiden Pole Freiheit und Sicherheit angemessen auszubalancieren. Z.B. hat der Sicherheitsrat der Vereinten Nationen einen sog. Sanktionsausschuss eingerichtet. Dieses Gremium verfasst Listen, auf denen natürliche Personen, aber auch Organisationen stehen, die aus der Sicht des Sanktionsausschusses mit den Tabliban oder al-Qaida in Verbindung stehen. Genannt werden derzeit knapp 500 Personen oder Organisationen, die EU hat das in ihr Gemeinschaftsrecht übernommen. Wenn Sie auf einer solchen Terrorliste stehen, können Sie im Grunde gar nichts mehr machen. Dann können Sie weder über Ihre Guthaben verfügen, noch dürfen Sie irgend etwas erwerben. Sie dürfen kein Geld in Empfang nehmen, und Sie dürfen auch das Land nicht mehr verlassen. ... Das Interessante ist, dass die Betreffenden, die auf eine solche Liste kommen, weder vorher angehört werden, noch dass ihnen die Gründe mitgeteilt werden, weshalb sie aufgeführt sind. Die zu Grunde liegenden Beweise werden nicht mitgeteilt, und es gibt keinen effektiven Rechtsschutz. ...

Im Hinblick auf den Grundrechtsschutz gegenüber EU-Recht hat das Bundesverfassungsgericht entschieden, dass es sich so lange zurückhält, wie auf europäischer Ebene gleichwertiger Grundrechtsschutz gewährleistet ist. Und das erfordert in aller Regel Individualrechtsschutz durch unab-hängige Gerichte, die mit angemessener Prüfungs- und Entscheidungsmacht ausgestattet sind. Daran fehlt es hier: Die einschlägigen Resolutionen des UN-Sicherheitsrats sehen derzeit keinen effektiven gerichtlichen Rechtsschutz für die Betroffenen vor. ... Es ist doch verständlich, dass bei der Aufstellung dieser Liste auch Fehler passieren können. Und wenn Sie als Betroffener dann nicht die Möglichkeit haben, dazu gehört zu werden, wenn Sie die Gründe nicht erfahren und auch keinen formalen Rechtsbehelf haben, dann sind Sie ziemlich schutzlos“ (Der Spiegel 3/2008, 26; SZ 14.01.2008,

6; 17.01.2008, 6; 24.01.2008, 8; www.tagesschau.de 13.11.2007; www.heise.de 11.11.2007; vgl. Antwort der Breg auf FDP-Anfrage v. 26.10.2007, BT-Drs. 16/6879; zu dem Thema ausführlich Frank Meyer/Julian Macke, Rechtliche Auswirkungen der Terroristenlisten im deutschen Recht, HRRS Dezember, www.HRR-Strafrecht.de).

Europa

Facebook kämpft mit dem Datenschutz

Seit September 2007 verhandelt die Internetkontaktbörse Facebook u.a. mit der Berlin Group, einer internationalen Arbeitsgruppe, die sich mit Datenschutzfragen im Telekommunik ationsbereich beschäftigt. Es geht um die Einführung europäischer Versionen, die sich wegen des Datenschutzes verzögert. Alexander Dix, Leiter der Berlin Group: „Vier Punkte bereiten uns noch Probleme: wie lange Daten gespeichert werden; das Mindestalter von 13 Jahren für die Registrierung [bei Facebook]; die Tatsache, dass die Nutzer zustimmen müssen, dass Facebook ihre Daten an seine Werbekunden weitergibt, und bessere Informationen über die Zugangsvoraussetzungen zu den Nutzerprofilen.“ Dix kann sich kaum vorstellen, dass Facebook die französische oder die deutsche Version eröffnet, bevor die Verhandlungen mit der Berlin Group abgeschlossen sind (www.ftd.de 16.11.2007; vgl. der Bericht zu StudiVZ auf S. XX).



Österreich

Polizei erhält neue Überwachungsrechte

Mit den Stimmen der Regierungsparteien SPÖ und ÖVP hat der österreichische Nationalrat am 05.12.2007 das Sicherheitspolizeigesetz (SPG), das Grenzkontrollgesetz und das Polizei kooperationsgesetz geändert, was der Polizei eine Fülle neuer Befugnisse bringt. Bei den Oppositionsparteien sorgte für besonderen Unmut, dass ein seit Oktober bekannter Entwurf wenige Stunden vor der Abstimmung umfassend abgeändert wurde, ohne dass die Öffentlichkeit oder gar auch nur der zuständige Innenausschuss zuvor informiert worden wäre. Daher stimmten auch die rechten Parteien FPÖ und BZÖ gegen die Neuerungen. Ablehnend votierten ebenso die Grünen sowie der über die SPÖ-Liste ins Parlament gewählte liberale Abgeordnete Alexander Zach.

Die Sicherheitsbehörden können nun ohne richterliche Genehmigung Telecom-Anbieter zwingen, Standortdaten und die internationale Mobilfunkteilnehmerkennung (IMSI) eines Handys preiszugeben, „wenn eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen besteht“. Ob diese Voraussetzungen tatsächlich vorliegen, wird aber nicht unabhängig geprüft. Die Behörden werden so technisch in die Lage versetzt, einen IMSI-Catcher zum Einsatz zu bringen, mit dem Telefonate von den betroffenen Anschlüssen aufgezeichnet und entschlüsselt werden können. Eine Herausgabepflicht besteht auch bzgl. Name und Anschrift von Nutzenden bestimmter IP-Adressen. Der Provider-Verband ISPA hat in letzter Sekunde eine Einschränkung auf „konkrete Gefahrensituationen“ und eine nachträgliche Information des Rechtsschutz beauftragten, der dem Innenministerium beigeordnet ist, erwirkt. Doch gibt es auch hier keine Vorab-Kontrolle, ob die Voraussetzungen wirklich vorliegen.

Neu eingeführt wurden Meldepflichten, zwangsweise Vorführungen und „präventive Anhaltungen“ für Personen, die gegen ein Betretungsverbot verstoßen haben oder im Zusammenhang mit einer bis zu zwei Jahren zurück liegenden Sportveranstaltung im In- oder Ausland „unter Anwendung von Gewalt einen gefährlichen Angriff gegen Leben, Gesundheit oder fremdes Eigentum“ begangen haben - eine Bestimmung kurz vor der Fußball-Europameisterschaft gegen Hooligans. Weiterhin wird eine öffentlich als „Sexualstraftäter-Datei“ diskutierte „Zentrale Analysedatei über mit beträchtlicher Strafe bedrohte Gewaltdelikte, insbesondere sexuell motivierte Straftaten“ eingerichtet. Der neue § 58d SPG regelt: „Es dürfen Informationen zu Tötungsdelikten, Sexualstraftaten unter Anwendung von Gewalt, Vermisstenfällen, wenn die Gesamtumstände auf ein Verbrechen hindeuten und zu verdächtigem Ansprechen von Personen, wenn konkrete Anhaltspunkte für eine mit sexuellem Motiv geplante mit Strafe bedrohte Handlung vorliegen, verarbeitet werden. Darüber hinaus dürfen tat- und fallbezogene Daten inklusive Spuren, Beziehungsdaten und Hinweise, Objektdaten und andere sachbezogene Daten, etwa zu Waffen oder Kraftfahrzeugen sowie Verwaltungsdaten verarbeitet werden.“ Daten über Opfer dürfen 20 Jahre, solche über Verdächtige auch ohne Verurteilung 30 Jahre gespeichert werden (Sokolov, www.heise.de 07.12.2007).

Frankreich

Sportlerin-Nacktfotos im Internet

Im Internet veröffentlichte Nackfotos der Schwimmerin Laure Manaudou haben in Frankreich für Empörung gesorgt und die Politik zu verbalem Eingreifen bewegt. Der Staatssekretär für Sport Bernard Laporte sprach von einem „skandalösen und feigen“ Vorgang und forderte: „Lasst Laure Manaudou sich bitte auf ihren Schwimmsport konzentrieren!“ Der Trainer und Bruder der 21-jährigen Sportlerin Nicolas Manaudou: „Wer immer das getan hat - ich hoffe, er wird dafür bezahlen.“ Manaudous ehemaliger Freund, der italienische Spitzenschwimmer Luca Marin, wies jegliche Schuld von sich: „Es hat sehr geschmerzt, die Bilder von ihr im Internet zu sehen. Es ist Schwachsinn, dass ich etwas damit zu tun haben könnte“ (SZ 21.12.2007, S. 29).



Niederlande

Sozialministerium späht Nachrichtenagentur aus

Bedienstete des niederländischen Sozialministeriums sind etwa ein Jahr lang illegal in das Computersystem der Nachrichtenagentur GPD eingedrungen. Mehr als 350mal hat sich das Ministerium gemäß dem stellv. GPD-Chefredaktuer Jos Timmer eingeloggt, um Texte zu lesen, welche die Arbeit des Ministeriums betreffen: „Sie sind fast täglich in unser Redaktionssystem reingegangen." Die beiden beschuldigten Sprecher des Ministeriums, ein Ehepaar, hatten vor ihrer Anstellung in Den Haag selbst bei der Nachrichtenagentur gearbeitet. Als zunächst die Frau ins Ministerium wechselte, konnte sie über das Passwort ihres Mannes verfügen. Später ging auch dieser zum Ministerium; sie benutzten die Codes ehemaliger Kollegen ohne deren Wissen.

Aufgefallen ist die Praxis, als ein Journalist der GPD ein Interview mit Sozialminister Donner geführt hatte. Die Redaktion hatte sich dann aber gegen die Veröffentlichung des Interviews entschieden und statt dessen ein Portrait des Ministers an die Regionalzeitungen ausgeliefert. Timmers: „Als schließlich ein Mitarbeiter des Ministeriums anrief und die Redaktion um einige Änderungen bat, dachten wir: Woher wissen die von dem Portrait? Es war ja noch gar nicht verschickt." In einem weiteren Fall versuchte das Sozialministerium Passagen eines Artikels zu ändern, in dem es um den Kündigungsschutz ging. Auch dieser Text war noch gar nicht an die abnehmenden Zeitungen weitergeleitet worden. Die seit dem Frühjahr 2007 amtierende große Regierungskoalition strebt eine heftig debattierte Lockerung des Kündigungsschutzes an. Die Nachrichtenagentur, die u.a. mit „Het Parool" und „Eindhovens Dagblad" mit einer Gesamtauflage von 1,7 Mio. zusammenarbeitet, erwägt nun rechtliche Schritte, so Timmers: „Wir sind überzeugt, dass mehr Leute im Ministerium von den Informationen in unserem Redaktionssystem und unseren Planungen wussten als nur die beiden Sprecher." Die niederländische Journalistengewerkschaft NVJ und die Vereinigung der Chefredakteure bezeichneten den Vorfall als eine „schwere Verletzung der Pressefreiheit". Auch die Nachrichtenredaktionen der niederländischen Sender RTL und NOS wollten prüfen, ob sich jemand unbefugt Zugang zu ihren Computersystemen verschafft hat (Nienhuysen SZ 06.11.2007, 7).

Großbritannien

Millionen Kindergelddaten abhanden gekommen

Der britischen Steuerbehörde sind sämtliche Daten der Empfänger von Kindergeld abhanden gekommen. Es geht um zwei CDs mit Angaben zu 7,25 Millionen Familien und insgesamt 25 Millionen Menschen - fast die halbe Nation. Die auf dem Postweg verschwundenen CDs enhielten Angaben zu Namen, Bankverbindungen, Adressen, Geburtsdaten und Sozial-versicherungsnummern. Schatzkanzler Alistair Darling, dem die Behörde untersteht, bestätigte, dass ein Finanzbeamter im nordenglischen Newcastle die beiden CDs am 18.10.2007 über den privaten Kurierdienst TNT an die Finanzkontrolle in London geschickt habe, wo sie aber nie angekommen seien. Der Angestellte behielt das zunächst für sich, weil er annahm, dass die Sendung wegen des Poststreiks aufgehalten worden sei. Erst am 08.11.2007 informierte er seine Vorgesetzten. Danach brach Panik aus. Darling hielt die Sache aber erst unter Verschluss, um den Banken Zeit zu geben, Sicherheitsvorkehrungen zu ergreifen. Die Polizei suchte vergeblich nach den CDs.

Die Daten waren zwar passwortgeschützt, aber nicht verschlüsselt. D.h. innerhalb von Minuten ist es für einen Experten möglich, an die Daten heranzukommen. Darling versicherte, es gebe keine Hinweise, dass die Daten in falsche Hände gelangt seien. Dennoch sollten die Betroffenen wachsam sein und auf ihre Kontobewegungen achten. Simon Davies von der London School of Economics und von Privacy International: „Die Informationen enthalten alles, was du brauchst, um Identitätsbetrügereien im Internet oder am Telefon zu begehen. Außer den Passwörtern ist alles da, um jemandem das Bankkonto zu plündern. Die meisten Leute benutzen einfache Passwörter wie den Namen ihres Kindes. Und der ist ja auf den CDs auch enthalten." Betrüger könnten mit den Informationen z.B. Handyverträge abschließen oder Kredite aufnehmen. Selbst wenn die CDs wieder auftauchen sollten, könne man nicht sicher sein, ob sie nicht kopiert worden sind."

Paul Gray, der Chef der Steuer- und Zollbehörde trat wegen dieses Vorgangs am 20.11.2007 zurück: „So habe ich mir meinen Abgang nicht vorgestellt". Gray hatte zuvor seit 1969 im Finanzministerium gearbeitet, von 1988 bis 1990 war er Margaret Thatchers Privatsekretär für Wirtschaftsangelegenheiten. Die Panne sei „katastrophal, beispiellos und unverzeihlich" meinte Darling, der Vorfall habe sein Vertrauen schwer erschüttert. Aber auch das Vertrauen der Bevölkerung in ihn ist erschüttert. Die Daten der Kindergeldempfänger sind offenbar regelmäßig auf Reisen. Bereits im März 2007 hatte die Steuerbehörde die beiden CDs nach London geschickt, aber die Finanzbehörde schickte sie wieder zurück. Nachdem sie im Oktober verloren gingen, schickte der Finanzbeamte ein drittes Mal - dieses Mal per Einschreiben. Ein Sprecher der Finanz-kontrolle erklärte, man habe die Adressen, Bankverbindungen und Namen der Eltern gar nicht verlangt, sondern wollte lediglich die Daten der Kinder mit den eigenen Unterlagen abgleichen. Chris Meyers von der IT-Firma Citrix: „Eine Menge Daten werden ohne Notwendigkeit verschickt. Wenn sie einmal weg sind, kann man das nicht ungeschehen machen. Computersysteme sollten so eingerichtet sein, dass Berechtigte Zugang zu den Informationen haben, ohne dass man die Daten per Post versenden muss." Der Datenschutzbeauftragte Richard Thomas: „Die Sache könnte kaum schlimmer sein, sie muss die Regierung wachrütteln. Wir haben vor diesen Gefahren seit mehr als einem Jahr gewarnt" (Sotscheck taz 22.11.2007, 17).




Großbritannien
Hunderttausende PatientInnendaten verloren

Hunderttausende PatientInnendatensätze von Erwachsenen und Kindern aus neun Verwaltungszentren des britischen Nationalen Gesundheitssystems (NHS) sind abhanden gekommen. Das britische Gesundheitsminsiterium teilte mit, es gebe keine Hinweise, dass sie in falsche Hände geraten seien. U.a. ist ein Datenträger mit Namen und Adressen von 160.000 Kindern verschwunden, der an ein Krankenhaus geliefert werden sollte. In einem anderen Fall sind archivierte Daten von KrebspatientInnen verloren gegangen, die vor 40 Jahren behandelt wurden. Andere Einzelheiten über die verschwundenen Daten wurden nicht bekannt gegeben. Da die Vorfälle auf lokaler Ebene behandelt würden, wisse das Gesundheitsministerium nicht, wieviel Personen davon betroffen sind. Die Datenverluste wurden anlässlich einer Sicherheitsüberprüfung von Behörden offenbar. Die Konservativen kritisierten, die Regierung sorge zu wenig für die Sicherheit, erhebe und speichere aber ständig neue Daten. Der Sprecher der Liberalen erklärte, „die ganze Kultur der Datenverwaltung muss sich bei den Behörden verändern“. In Großbritannien wird eine zentrale Datenbank mit allen Patientenakten aufgebaut, die für Krankenhäuser und Arztpraxen zugänglich sind. Der Verlust ist nicht der erste: Kurz zuvor sind Kindergelddaten abhanden gekommen (s.o.). Mitte Dezember 2007 wurde bekannt, dass dem Verkehrsministerium durch Outsourcing der Datenspeicherung an eine US-Firma eine Festplatte mit Datensätzen von 3 Millionen FahrschülerInnen verloren ging (Telepolis, www.heise.de 23.12.2007).

Großbritannien
Datenverlust beim Militär

Das britische Militär musste eingestehen, am 10.01.2008 personenbezogene Daten von 600.000 NachwuchssoldatInnen verloren zu haben. Ein Jungoffizier der Royal Navy hatte die Namen, Pass- und Versicherungsnummern sowie Angaben zum Familienstand von Rekruten und anderen BewerberInnen für den Militärdienst auf seinem Laptop gespeichert und über Nacht auf dem Beifahrersitz seines Autos auf einem bewachten Militärgelände liegen lassen. Am nächsten Morgen fand er seinen Wagen aufgebrochen vor und der Laptop war gestohlen. Wie der Täter das Notebook vom Militärgelände herausschmuggeln konnte, ist bislang nicht geklärt. Unter den gestohlenen Daten befinden sich auch Informationen über 3.500 Bankverbindungen. Diese Betroffenen wurden mit einem Eilschreiben des Verteidigungs-ministeriums informiert. Zudem meldete ein Autofahrer den Fund von hunderten Dokumenten an einem Straßenrand in Devon. Dabei handelte es sich um Anträge auf Renten und Arbeitslosengeld sowie Bankauskünfte und Kopien von Pässen. An gleicher Stelle hatte er Ende 2007 schon eine ähnliche Entdeckung gemacht. David Miliband räumte in der BBC ein, seine erste Reaktion nach der neuen Panne sei der Ausruf „Oh, nein!“ gewesen. Wegen dieser vierten Datenpanne innerhalb weniger Monate (s.o.) steht die britische Regierung von Gordon Brown wegen des schlampigen Umgangs mit sensiblen Daten unter steigendem Druck (www.heise.de 19.01.2008; SZ 21.01.2008, 7).

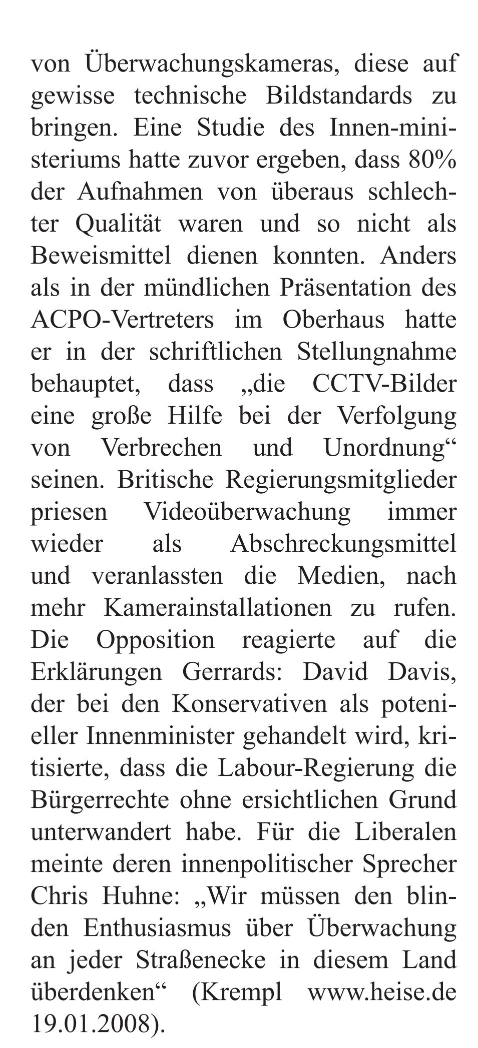
Großbritannien
Brown für noch schärfere Anti-Terror-Gesetze

Der neue britische Premierminister Gordon Brown hat zu Beginn der Sitzungsperiode des Parlaments verschärfte Anti-Terror-Gesetze angekündigt. In der von Königin Elizabeth II. verlesenen Regierungserklärung stellte Brown am 06.11.2007 eine Gesetzesinitiative in Aussicht, die der Polizei und den Geheimdiensten einen leichteren Austausch von Informationen ermöglichen soll. Die Pläne sehen zudem vor, dass Ermittler Verdächtige künftig auch nach der Anklageerhebung weiter befragen dürfen, was bisher nur eingeschränkt möglich ist (SZ 07.11.2007, 9).

Großbritannien
Polizei räumt eklatante Schwächen der Videoüberwachung ein

Graeme Gerrard, bei der britischen Association of Chief Police Officers (ACPO) für Videoüberwachung zuständig, räumte bei einer parlamentarischen Anhörung ein, dass die in Großbritannien bis zur Totalüberwachung reichende Videoüberwachung Gewaltverbrechen und spontan begangene Straftaten nicht verhindert. Er bestätigte, dass in anderen Ländern großes Erstaunen bestehe, in welchem Ausmaß in seinem Land „Closed Circuit Television“ (CCTV, also Videoüberwachung) eingesetzt wird. Die Abschreckungswirkung sei sehr gering. Der Experte der Vereinigung der lokalen Polizeichefs gab zu, dass die Öffentlichkeit über die Effizienz der elektronischen Augen „in die Irre geführt“ worden sei. Gemäß Schätzungen waren 2007 im Vereinigten Königreich 4 Mio. Überwachungskameras für viele hundert Millionen Pfund installiert. Großbritanniens Datenschutzbeauftragter Richard Thomas sprach deswegen vom „Schlafwandeln“ hinein in die Überwachungsgesellsch aft. Vor allem bei spontan, z.B. im Trunkenheitszustand begangenen Verbrechen und bei antisozialem Verhalten habe sich der technische Beschattungskomplex als nutzlos herausgesetellt. Wenn Menschen in den Innenstädten nachts ihrem Ärger Luft machen wollten, würden sie nicht auf über ihnen aufgehängte Kameras achten. Deren Aufnahmen könnten dann allenfalls noch bei der späteren Strafverfolgung helfen.

Wirkungsvoller sei die Videoüberwachung bei Parkplätzen, wo es um die Verhinderung von Autodiebstahl geht. Dort würden die potenziellen Täter „rational“ handeln und beim Erkennen von CCTV-Anlagen eher von einem Wagenaufbruch absehen. Gerrard forderte eine Verpflichtung für die Betreiber



von Überwachungskameras, diese auf gewisse technische Bildstandards zu bringen. Eine Studie des Innen-ministeriums hatte zuvor ergeben, dass 80% der Aufnahmen von überaus schlechter Qualität waren und so nicht als Beweismittel dienen konnten. Anders als in der mündlichen Präsentation des ACPO-Vertreters im Oberhaus hatte er in der schriftlichen Stellungnahme behauptet, dass „die CCTV-Bilder eine große Hilfe bei der Verfolgung von Verbrechen und Unordnung" seinen. Britische Regierungsmitglieder priesen Videoüberwachung immer wieder als Abschreckungsmittel und veranlassten die Medien, nach mehr Kamerainstallationen zu rufen. Die Opposition reagierte auf die Erklärungen Gerrards: David Davis, der bei den Konservativen als potenieller Innenminister gehandelt wird, kritisierte, dass die Labour-Regierung die Bürgerrechte ohne ersichtlichen Grund unterwandert habe. Für die Liberalen meinte deren innenpolitischer Sprecher Chris Huhne: „Wir müssen den blinden Enthusiasmus über Überwachung an jeder Straßenecke in diesem Land überdenken" (Krempl www.heise.de 19.01.2008).



Großbritannien

Kommt der implantierte GPS-RFID-Chip für Straftäter?

Die britische Regierung erwägt die Implantation von RFID-Chips bei verurteilten Straftätern, um die überfüllten Gefängnisse zu entlasten und die Zahl der Hausarreste zu erhöhen. Die Chips sollen den Aufenthalt der Betroffenen per GPS in Echtzeit per Satellit lokalisieren. Zuvor hatte der britische Polizeiverband ACPO gefordert, verurteilten Pädophilen und anderen Sexualtätern GPS-Sender zu implantieren, um zu verhindern, dass sie in die Nähe von „verbotenen Orten wie Schulen und Kindergärten" gehen. Seit 1997 wuchs die Zahl der Gefängnisinsassen von 60.000 auf 80.000. 2007 ist die Zahl der Menschen, die in Gefängniszellen gesteckt wurden, um das 1,3fache gestiegen. Großbritannien hat verhältnismäßig die meisten Strafgefangenen in Europa. Die Regierung plant für Milliarden von Euro drei neue Großgefängnisse und Platz für Tausende von Insassen. Derzeit sind schon mehr als 17.000 verurteilte Straftäter und Verdächtige unter Auflagen und elektronischer Überwachung im Hausarrest untergebracht. 2000 der Betroffenen verhindern jährlich die damit verbundene Überwachung, indem sie die bislang verwendeten elektronischen Fußfesseln manipulieren oder entfernen. Die Übertretungen der Auflagen sind von 2005 auf 2006 um 280% angewachsen. Das Projekt „Gefängnis ohne Gitter" mit satellitenüberwachten Fußfesseln stieß zudem in Städten auf Probleme, weil die Überwachten in der Nähe von großen Gebäuden nicht mehr erfasst werden konnten. Um nun zu verhindern, dass die Überwachten sich das GPS-Gerät entfernen, wird nun im britischen Justizministerium überlegt, die Elektronik unter die Haut zu implantieren. Dadurch könne überprüft werden, ob diese sich an den auferlegten Hausarrest halten.

Bewährungshelfer und Menschenrechtsgruppen lehnen die Maßnahme ab. Shami Chakrabarti, Direktorin der Bürgerrechtsorganisation Liberty, erklärte, das Implantieren von Chips sei schlimmer als die elektronische Fußfessel: „Straftäter auf diese Weise zu entwürdigen, bringt nichts für die Wiedereingliederung und nichts für unsere Sicherheit, da einige unweigerlich eine Möglichkeit finden werden, diese Technik auszutricksen." Harry Fletcher, stellv. Leiter der Nationalen Vereinigung der Bewährungshelfer (NAPO) lehnt die Chips auch ab, mit denen man Menschen wie Haustiere oder Fleischstücke identifiziere (Telepolis www.heise.de 14.01.2008).

Schweden

SportlerInnen schlagen Chipimplantate für Dopingkontrolle vor

Schwedens bekannte LeichtathletInnen Carolina Klüft und Stefan Holm machten Vorschläge zur Überwachung von SpitzensportlerInnen, um dem Dopingproblem Herr zu werden. Olympiasiegerin Carolina Klüft, seit Sommer 2001 bei Siebenkampf-Wettbewerben unbesiegt, meinte: „Ich habe ja schon öfter vorgeschlagen, wir sollten Computerchips unter der Haut tragen. Aber vielleicht reicht es auch, dass wir ein GPS-System bei uns haben, damit man zu jeder Zeit weiß, wo wir sind und für Dopingtests erreicht werden können." Hochsprung-Olympiasieger Holm assistiert: „Es klingt zwar brutal, aber es scheint mit eine gute Lösung zu sein, um falsche Verdächtigungen zu vermeiden. Ohne Chip gibt es keine hundertprozentige Sicherheit." Etliche SpitzenathletInnen hatten zuletzt Verwarnungen erhalten, weil sie für Dopingkontrollen nicht auffindbar gewesen seien. Sie müssen die Anti-Doping-Agenturen ständig über ihren Aufenthaltsort informieren. Bei Erstvergehen drohen Verwarnungen, ab dem zweiten Missed Test werden Sperren ausgesprochen (SZ 21.12.2007, 29).

Liechtenstein

Bankgeheimnis wird zwecks Korruptionsbekämpfung gelockert

Die liechtensteinische Regierung in Vaduz teilte mit, dass sie die Ratifikation der UN-Konvention zur Korruptionsbekämpfung für Anfang 2008 vorbereitet, was zur Folge hätte, dass bei bestimmten Schmiergeldzahlungen trotz des Bank-geheimnisses internationale Rechtshilfe gewährt würde. Keine Rechtshilfe wird gewährt, wenn ein Privat-Unternehmen eine andere Privatfirma oder -person besticht. Derartige Korruption ist derzeit nach dem Recht Liechtensteins nicht strafbar. Die UN-Konvention erfasst die Bestechung von Beamten und Amtspersonen. Liechtenstein hatte das Abkommen bereits 2003 unterzeichnet, wollte aber offensichtlich Treuhändern und Banken bis zur Ratifikation Zeit geben, um sich auf die strengeren Vorschriften einzustellen. Konkret bedeutet dies, dass bei einem begründeten Anfangsverdacht liechtensteiner Treuhänder Auskunft geben müssen

über die wirtschaftlich Berechtigten, die hinter einer Stiftung stehen, und dass diese Auskünfte an ein anderes Land weitergebeen werden. Auch Konto-Bewegungen und ähnliche Informationen können künftig an Drittstaaten wei-ter-gegeben werden. Bislang setzt dies schwerwiegendere Vorwürfe voraus. Der Siemens-Schmiergeldskandal kam z.B. ins Rollen, weil lichtensteiner Behörden Verdacht auf Geldwäsche und Untreue schöpften.

Bereits gegenwärtig unterliegen Treuhänder und Banken im Fürstentum einer - der Schweiz vergleichbaren - Sorgfaltspflicht, wonach sie ihre KundInnen kennen müssen und keine Gelder zweifelhafter Herkunft entgegen nehmen dürfen. Dies entspricht nach Ansicht der Regierung in Vaduz weitgehend internationalen Standards. Zu diesem Ergebnis dürfte auch eine Beurteilung durch den Internationalen Währungsfonds kommen, die in Bälde verabschiedet werden soll. Das Bankgeheimnis gilt im Wesentlichen nur noch in Erbschafts- und Steuerangelegenheiten, doch gibt es auch hier Ausnahmen. So hat das Fürstentum mit den USA ein Abkommen geschlossen, das einen Informations-austausch beim Verdacht auf bestimmte Steuerdelikte möglich macht. Bisher hat, so vaduzer Regierungskreise, dieses Abkommen aber wenig praktische Bedeutung erlangt. Mit der EU verhandelt Liechtenstein auf Druck von Brüssel über ein sog. Betrugsabkommen. Dabei geht es um die Aufhebung des Bankgeheimnisses beim Verdacht auf Hinterziehung von Mehrwertsteuer, Zöllen und anderen indirekten Steuern. In Liechtenstein sind dies keine Straftaten, weshalb auch in diesen Fällen keine Rechtshilfe geleistet wird. Wenn Liechtenstein der Schengen-Vereinbarung beitritt, womit für 2008 gerechnet wird, wird es zu weiteren Verschärfungen kommen. Dann wird der Zwergstaat zwar nicht bei einfacher Steuerhinterziehung, wohl aber bei Steuerbetrug Rechtshilfe leisten (Zitzelsberger SZ 07.12.2007, 6).



USA

FBI plant weltweit größte Biometrie-Datenbank

Im Januar 2008 hat die US-amerikanische Bundespolizeibehörde (FBI) einen Zehnjahresvertrag mit einem Umfang von insgesamt einer Millarde Dollar (690 Mio. Euro) vergeben, um ein biometrisches Informationssystem zur Identifizierung von Verdächtigen „deutlich auszuweiten“. „Next Generation Identification“ erfasst in einem Datenzentrum in Clarksburg/ WestVirginia Personen innerhalb und außerhalb der USA anhand charakteristischer Körpererkennungsmerkmale. Die Datenbank soll im Jahr 2013 in der Lage sein, so FBI-Abteilungsleiterin Kimberley Del Greco, Anfragen anhand eines Datenmixes aus Finger- und Handballenabdrücken, Iris- und Gesi chtserkennungsmerkmalen abzugleichen. So soll ein Sicherheitsbeamter am Flughafen in Sekundenschnelle erfahren können, ob die Person, deren Hände soeben überprüft werden, in der Liste von gesuchten Verdächtigen, Kriminellen, Terroristen usw. auftaucht. Erwogen wird auch die Erfassung der Geh- und der Sprachmuster zu Identifzierungszwecken. Thomas Bush vom kriminalistischen Informationsdienst des FBI: „Größer, schneller, besser - darum geht es“.

Das neue System soll sich nicht nur durch zusätzliche biometrische Merkmale quantitativ und qualitativ auszeichnen, sondern auch durch eine verbesserte Kommunikation zwischen verschiedenen Datenbanken. Mit dem Service „Rap-Back“ würde das FBI auf Anfrage von Arbeitgebern Angestellte auf kriminelle Hintergründe überprüfen, die Unternehmen würde über Treffer benachrichtigt und die biometrischen Angaben der Betroffenen blieben gespeichert. Derzeit betreffen gemäß einem Bericht der „Washington Post“ 55% solcher Anfragen Zivilpersonen, die in sicherheitsempfindlichen Positionen tätig sind, sich bei der Regierung bewerben oder mit Kindern oder älteren Menschen zu tun haben.

Bereits jetzt speichert die FBI-Datenbank 55 Millionen elektronische Datensätze mit Fingerabdrücken. Verfügbar sind u.a. die biometrischen Daten von 1,5 Millionen IrakerInnen, AfghanInnen und anderen AusländerInnen. Täglich werden 100.000 Anfragen mit diesen Daten abgeglichen. 900.000 Strafverfolger dürfen in den USA auf diese Fingerabdruckdatenbank zurückgreifen. Das FBI verspricht, den Zugang zu der Datenbank genau zu überwachen. Dennoch ist klar, dass die Risiken für die BürgerInnen wachsen. Das System sei nicht verlässlich, heißt es. Informationen in der Datenbank seien oft fehlerhaft oder ungenau. Das FBI bestätigt, dass es im Vornhinein schwierig ist zu bestimmen, welche Informationen fehlerhaft sind. Liegt ein Fehler vor, so ist es für die Betroffenen sehr schwierig, diesen korrigieren zu lassen. Dennoch sieht Bush vom FBI die Daten hinreichend geschützt: „Wir haben strikte Gesetze, wer da rein darf und wie die Daten geschützt werden.“ Jede Anfrage werde verzeichnet. Alle Behörden mit Zugang zu der Datenbank würden alle drei Jahre überprüft. Bürgerrechtsanwälte warnen dagegen vor einer „dauernd angeschalteten Überwachungsgesellschaft“ (Pany www.heise.de 22.12.2007; SZ 24.-26.12.2007, 1; KN 24.12.2007, 6).

USA

Wall Street Journal nutzt Internet als Pranger gegen Siemens

Das Wirtschaftsblatt „Wall Street Journal“ nahm sich die Freiheit, die Liste der angeblichen Adressaten von Schmiergeldzahlungen des Münchner Siemens-Konzerns in drei Länder zu veröffentlichen. Damit wurden Urteile und Beschlüsse deutscher Gerichte mit Namensnennung veröffentlicht, was nach deutschem Recht i.d.R. nur geschwärzt erfolgen darf. Aus rechtlichen Gründen erfolgte eine wortgetreue Übersetzung, mit der der Charakter von Gerichtsdokumenten gewahrt werden soll. Bei möglichen Klagen der Betroffenen erhofft sich das Blatt so presserechtlich eine bessere Position. In nigerianischen Medien haben einige der Betroffenen, deren Namen bei Vernehmungen genannt wurden



oder die sich in Firmenunterlagen finden, je-gliche Bestechnung bestritten. Ein ehemaliger Telekommunikationsminister Nigerias, der das Amt in den Jahren 1994 bis 1998 innehatte, taucht in der Münchner Liste mit einer angeblichen Schmiergeldzahlung am 08.08.2002 auf, beteuert aber, nichts erhalten zu haben (SZ 20.11.2007, 20).

Iran

Internet-Nutzende verhaftet

„Reporter ohne Grenzen" (ROG) meldeten, dass im Iran am 16.12.2007 zwei Dutzend Internetcafés geschlossen und 23 Nutzende, darunter 11 Frauen, verhaftet worden sind. Der Vorwurf ist „unmoralisches Verhalten", ohne dass dies konkretisiert wurde. Im Iran unterliegt das Internet einer strengen Zensur. ROG: „Die Linie der Regierung in Sachen freie Meinungsäußerung radikalisiert sich weiter, vor allem, wenn Frauen betroffen sind. Die Gründe für die Festnahmen sind extrem vage" (Meusers www.spiegel.de 19.12.2007).



China

Cyber-Stalking greift um sich

Internet-Hetzjagden, die ins reale Leben übergreifen, sog. „Cyber-Stalking", scheinen sich in China immer größerer Beliebtheit zu erfreuen. So musste sich 2006 ein junger Mann, der unter dem Internet-Namen „bronzefarbener Schnurrbart" im Netz aktiv war, real verstecken, nachdem Tausende Surfer dem Liebhaber einer verheirateten Frau angedroht hatten, „den Kopf abzuschlagen". Es kommt immer wieder zu telefonischen Morddrohungen gegen Ausländer, denen zuvor im Internet „Beleidigung der chinesischen Nation vorgeworfen wurde.

Die Süddeutsche Zeitung berichtete nun von der Hexenjagd gegen den 31jährigen Pekinger Yin Qi, Abteilungsleiter in der pekinger Niederlassung der britischen Firma Quantel, einem Hersteller digitaler TV-Ausrüstung. Yins Probleme begannen, als seine Ehefrau Zhang Meiran im Internet über seine Exfrau herzog. Unter dem Tarnnamen „Candy" machte sich die neue Ehefrau in gehässiger Weise über die geschiedene Ehefrau lustig. Die Ex hatte bei ihrer Scheidung von Yin die gemeinsame Wohnung erhalten, was der neuen Ehefrau offenbar nicht passte. Zhang Meiran alias „Candy": „Sie ist nur eine billige Henne, die beim Sex nur eine einzige Position kennt". Dies führte dazu, dass sich erst Hunderte, dann Tausende und Zehntausende im Internet über das Ehepaar Yin und Zhang im Internet aufregten, z.B.: „Und du glaubst, du bist hübsch? Schau dir dein Gesicht an, flach wie ein indischer Pfannkuchen". Yin Qi sei unmoralisch, weil er schon während seiner ersten Ehe ein Verhältnis mit Zhang Meiran hatte, befanden selbst ernannte Moralwächter im Internet. Irgendjemand wühlte und veröffentlichte schließlich die Namen des Ehepaares, ihre Personalausweisnummern, Adressen, Fotos, Arbeitergeber und Telefonnummern. Danach liefen in den Büros von Yins Firma die Telefone heiß. Die Anrufenden verlangten, dass die Firma den Chinesen entlässt. Der zur Zielscheibe gewordene Yin Qi musste sich verleugnen lassen (Bork SZ 20.11.2007, 10).

USA

Videokameras aus Schulen direkt zur Polizei

In drei öffentlichen Primärschulen des Kreises Demarest in New Jersey wurden aus Sorge vor möglichen Gewalttaten wie Amok laufenden Schülern zusätzlich zur bestehenden Videoüberwachung in den Eingangsbereichen jeweils sieben bis neun neue Überwachungskameras installiert, auf die die Polizei direkt von ihrem Hauptquartier oder von den Laptops in den Fahrzeugen aus zugreifen kann. Der Polizeichef: „Die Schulen sollen die sichersten Orte sein. Nichts ist wertvoller als unsere Kinder". Die Kameras wurden in Turnhallen, Cafeterien, Gängen, auf Spielplätzen und in Eingangsbereichen aufgestellt. Die Klassenzimmer sind noch überwachungsfrei. Um die Privatsphäre zu wahren, wird auf die Tonaufnahme verzichtet. Die Bilder werden einen Monat lang gesepichert. Die Polizei kann auf Monitoren gleichzeitig 16 verschiedene Kameras beobachten: „Ein Polizeioffizier hat 17 Augen an vielen Orten." Für den Schuldirektor haben die Kameras einen weiteren Zweck. Weil die Bilder mit Zeitangabe für einen Monat gespeichert werden, sollen sie nicht nur vor kriminellem, sondern auch schlechtem Verhalten abschrekken. An einer weiteren Schule ist ein Kamerasystem geplant, das erkennen soll, wenn sich jemand in einer Notlage

China

Handy-Filmer wurde erschlagen

Ein Mann wurde von Polizisten erschlagen, weil er deren brutales Vorgehen gegen Demonstranten mit seiner Handy-Kamera festhielt. Die amtliche Nachrichtenagentur Xinhua berichtete, dass der 41jährige Wei Wenhua filmte, wie die Polizisten aus Tianmen gegen Dorfbewohner vorgingen, die gegen eine Müllkippe demonstrierten. 24 Polizisten wurden demnach wegen Fehlverhaltens festgenommen (SZ 10.01.2008, 8).

Technik-Nachrichten

Google offeriert Handy-GSM-Ortungsdienst

Der Suchmaschinenbetreiber Google hat eine Handy-Software vorgestellt, mit der man auch ohne GPS grob ermitteln kann, wo man gerade ist. Dies wird ermöglicht über BenutzerInnen von Google Maps, die ein Telefon mit GPS-Unterstützung besitzen. Wann immer sie die Maps-Software verwenden, werden die zehnstelligen Kennziffern der Mobilfunkmasten mit der Position zusammengebracht, die per GPS bestimmt wurde. Das Handy erkennt technisch, welche Mobilfunkmasten in seiner Nähe sind. Google weiß aus den gesammelten Daten der GPS-Handybenutzenden, wo diese stehen und errechnet aus Informationen wie der Signalstärke die ungefähre Position. Je mehr Masten in der Nähe sind, umso exakter wird die Position bestimmt. Während GPS auf einige Meter genau ist, liefert die Funkmastenmethode allerdings nur eine grobe Schätzung. In dünn besiedelten Gebieten mit wenigen Funkmasten kann der errechnete Aufenthaltsbereich an die zwei Kilometer groß sein.



Um den Dienst nutzen zu können, benötigt man ein Handy, das Java-Programme ausführen kann. Als geeignet bezeichnet Google u.a. Geräte des Herstellers Blackberry, Geräte mit Symbian-60-Betriebssystem sowie mit jüngeren Versionen von Windows Mobile. Ratsam sei ein Handyvertrag mit einem Festpreis für Datenübertragung, da für die Datendarstellung vergleichsweise viel Daten übermittelt werden. Auch ohne UMTS geht das aber einigermaßen schnell. Google hat angekündigt, in diesen Dienst künftig auch Werbung zu integrieren. Die Ortung von Mobiltelefonen findet eine Vielzahl von Anwendungen. Dabei können die Masten und die Entfernung hiervon detektiert werden. Es gibt Firmen, die anbieten, Familienangehörige so zu lokalisieren. Diese Technik wurde dem Kopf der Entführer des hamburger Millionärs Jan Philipp Reemtsma zum Verhängnis: Als er ein Rockkonzert in Agentinien besuchte und sein Mobiltelefon nutzte, konnten die Fahnder zugreifen (Martin-Jung SZ 01./02.12.2007, 24).

Samsung stellt RFID-Empfänger für Mobilgeräte vor

Samsung hat einen RFID-Empfänger für Handys oder Smartphones entwickelt, mit dem sich Auskünfte zur RFID-markierter Ware auf dem Handy anzeigen lassen. Nutzende können z.B. auf der Basis der verfügbaren RFID-Technik Informationen über Kleidungsstücke in Schaufenstern, von Plakaten zu Kinofilmen oder von Ausstellungstücken in Museen besorgen, sofern diese Objekte mit RFID-Transpondern ausgestattet wird. Der Single-Chip-Transceiver mit einer Größe von 6,5 zu 6,5 mm kommuniziert mit RFID-Tags im UHF-Band bei 900 MHz. In dem Tag-Reader steckt neben der HF-Elektronik ein Prozessor, Speicher und ein Sender, um passive Transponder mit der Ansprache zugleich mit Energie für deren Antwort zu versorgen. Vor der Implementierung des RFID-Lesers in kommenden Geräten sollen nachrüstbare Adapter für bereits verfügbare Mobilgeräte die Nutzung des Services ermöglichen. Nach Angaben des Marktforschungsunternehmens AoA Group soll die Nachfrage von mobilen RFID-Chips von 26,9 Mrd. US-Dollar im Jahr 2007 auf 701 Mrd. Dollar im Jahr 2010 ansteigen (www.heise.de 29.11.2007).

Motorola analysiert Handy-Kommunikationsinhalte für Werbezwecke

Motorola arbeitet an einer Technologie, die die Kommunikationsinhalte von Handynutzenden nach werberelevanten Schlüsselbegriffen, z.B. „Essen gehen" oder „Hunger" durchsucht und dann - in Verbindung mit der Standortangabe - passende Werbung, z.B. für Restaurants in der Nähe zusendet. Derzeit konzentriert sich die Entwicklung noch auf Textnachrichten. Motorolas Marketingchef Kenneth Keller erläuterte aber, dass die Technik auch geeignet ist, menschliche Sprache zu untersuchen. Er räumte ein, dass solche Dienste erhebliche Auswirkungen auf die Privatsphäre und den Datenschutz der Mobilfunkkunden habe. Daher werde das Angebot als „Opt-in"-Modell ausgestaltet. Wer seine Kommunikation derart scannen lässt, könne z.B. durch Freiminuten belohnt werden.

Simon Davies, Direktor der in London ansässigen Bürgerrechtsorganisation Privacy International (PI), befürchtet, dass sich Mobilfunkanbieter einige Lockmittel einfallen lassen, damit die KundInnen der Werbeoption „freiwillig" zustimmen. Am Ende laufe es aber stets darauf hinaus, dass die KundInnen, die nicht mitmachen, verschlechterte Konditionen hinnehmen müssten. Schon jetzt wird verstärkt versucht, Handy-KundInnen mit „Mobile Marketing" zu beschicken. Seit Herbst 2007 lockt die vom ehemaligen Nokia-Präsidenten Pekka Ala-Pietilä mitbegründete Firma Blyk gezielt Jugendliche in Großbritannien mit 217 Gratis-SMS und 43 Freiminuten pro Monat, wenn sie dem Empfang von Reklame per MMS zustimmen. Deren Inhalt ist abhängig von den Angaben, die die Nutzenden in einem Online-Formular machen. Marktforschende prognostizieren für den Markt des Mobile Marketing ein großes Wachstum, weil damit konsumfreudige Teenager angesprochen werden könnten, die über traditionelle Werbeträger nur unterdurchschnittlich erreicht werden. Gemäß einer Studie des Marktforschungsinstituts Informa umfasst der Handy-Werbemarkt im Jahr 2011 voraussichtlich ein Volumen von 11 Mrd. US-Dollar. Nach Ansicht von erfahrenen Mobilvermarktern sollte das Potenzial des Mobile Marketing aber nicht durch „peinliche Werbeformen" vergeudet werden. So meinte der Chef der Grey Global Group, Mobile Marketing brauche viele Pull- und vertrage nur wenig Push-Elemente. Die KonsumentInnen hätten eine Abneigung gegen lästige, da ungefragte und ohne Bezug versandte Botschaften, über welches Medium auch immer (www.heise.de 29.10.2007).



Mobiltelefonie-Daten für „Reality Mining"

Sandy Pentland, Professor für Medienwissenschaften am MIT/USA, startete 2004 einen Versuch zur Erfassung der Internaktionen zwischen 100 Versuchspersonen - Studierende und Institutsangehörige, denen Hands mit besonderer Software zur Verfügung gestellt wurde. Basierend auf den Gesprächsdaten und dem mittels Bluetooth erfassten Abstand zwischen den Geräten, entwickelten Pentland und sein Kollege Nathan Eagle digitale Abbilder sozialer Netzwerke. Dabei erwies sich, dass die erfassten Informationen deutlich genauer waren als ein vorher über Befragungen aufgestelltes Interaktionsmodell der Testpersonen. Pentland entwickelt auf diese Weise eine sog. „Reality Mining"-Technologie, deren Ziel die Erfassung und Verarbeitung von Daten aus der Lebenswirklichkeit ist. Sein Ziel ist es, der an sich „dummen" IT-Infrastruktur etwas über unser Sozialverhalten beizubringen: „All diese Web-2.0-Dienste sind ja ganz nett, aber man muss immer alles erst eintippen. Dadurch sind die Daten niemals auf dem neuesten Stand. Reality Mining erkennt diese Muster in unserem Leben." Das Handy sei besonders gut geeignet, weil es an sich schon so viele Sensoren mitbringt, etwa Bluetooth oder die Erfassung der Funkzelle sowie Beschleunigungsmesser im iPhone. Dass diese „ultimative Datenerfassungsmaschine" ein Privatsphärenproblem darstellt, sieht Pentland. Klar sei aber, dass die neuen Funktionen kommen: „Wir brauchen eine neue Übereinkunft darüber, wie sie eingesetzt werden. Es hilft nichts, einfach den Kopf in den Sand zu stekken" (Technology Review www.heise.de 17.01.2008).

Microsoft lässt Nutzenden-Totalüberwachungssoftware patentieren

Forschende des Software-Konzerns Microsoft wollen ein Kontrollsystem per Patent schützen lassen, mit dem Blutdruck, Herzfrequenz, Gesichtsausdruck, Hautwiderstand, Muskelspannung, Gehirnströme und vieles mehr von Büromitarbeitenden per Funksensoren und auf andere Weise erfasst und kontrolliert werden, um festzustellen, wie gestresst Computeranwender sind und wie Mitarbeiter-Leistungen gemessen und Arbeitsprozesse effizienter gemacht werden können. Das System zur „Überwachung von Gruppenaktivitäten" kann „automatisch Frustration oder Stress bei Computeranwendern ausmachen". Dazu kontrolliert ein Programm, was der Anwender am Computer gerade macht und vergleicht diese Daten mit den Angaben von drahtlos vernetzten Sensoren, die Blutdruck, Mimik, Körpertemperatur usw. kontrollieren. Der Patentantrag für dieses Kontrollsystem wurde von acht Forschenden zugunsten von Microsoft Mitte 2006 beim US-Patentamt eingereicht. Erst 18 Monate später wurde er öffentlich gemacht. Im Patentantrag zählen die Forschenden folgende möglichen Anwendungen auf: Herausfinden, wann Anwender Hilfen beim Erfüllen bestimmter Aufgaben brauchen, andere Anwender aufspüren, die einem Anwender bei seiner Aufgabe helfen oder sie für ihn übernehmen können, Probleme bei Arbeitsabläufen ausmachen, Leistung von Anwendern vergleichen.

Es ist völlig offen, ob Microsoft aus dem sehr abstrakten Patentantrag mit der Dokumentnummer 20070300174 ein derartiges Produkt plant oder je planen wird. Eine Microsoft-Sprecherin wollte den Patentantrag selbst nicht kommentieren, meinte aber, Microsoft sei stolz auf seine weltweit 7000 zugestandenen Patente. Eine Kommentierung erfolge aber nicht, weil in dieser Phase alle in den Dokumenten gemachten Angaben noch geändert werden könnten. Microsoft erklärte, dass es die Privatsphäre sehr ernst nähme. Besonders wichtig sei die Zustimmung der Nutzenden zur Auswertung ihrer Daten. Datenschützer kritisieren das Patentverfahren, so Padeluun vom FoeBuD: „Wenn jemand seine Mitarbeiter bis zum Puls kontrolliert, ist das nicht hinzunehmen. Das mag in der Raumfahrt üblich sein, aber im Büro verstößt es gegen die Moral." Die britische Zeitung „Times" spricht von einer Big-Brother-Software (www.spiegel.de 16.01.2008; Schrader SZ 17.01.2008, 1).

Geschäft mit Überwachungsdrohnen boomt

Die Firma Microdrones im sauerländischen Kreuztal hat inzwischen rund 300 mit Überwachungskameras ausgestattete Hightech-Minihubschrauer weltweit verkauft - Tendenz steigend. Kunden sind u.a. Sicherheitsbehörden in China. Um auf etwaige Vorkommnisse bei den im August 2008 beginnenden Olympischen Spielen schneller reagieren zu können, plant Peking eine verstärkte Überwachung aus der Luft. Innenminister Albrecht Buttolo (CDU) will die „fliegenden Augen" im Rahmen einer Großoffensive gegen Fußball-Randalierende im Freistaat Sachsen einsetzen. Nach vielen blutigen Krawallen im Umfeld von Fußballspielen will das Innenministerium „zusätzliche Beweissicherungstechnik im Umfang von rund 300.000 Euro" sowie „fliegende Kameras" anschaffen. Für Hightech-Überwachung aus der Luft sind Ausgaben in Höhe von 65.000 Euro für wohl vier Drohnen vorgesehen. Gemäß den Angaben von Bernd Rohde von Microdrones kostet ein durchschnittliches System vom Typ MD4-200 13.000 bis 14.000 Euro.

Der MD4-200 ist mit vier gegenläufigen Rotoren ausgestattet und arbeitet mit bis zu neun verschiedenen Prozessoren. Eingesetzt werden können vier unterschiedliche Kameras, darunter eine 10-Megapixel-Digitalkamera von Pentax für Einzelbilder sowie eine Panasonic Lumix für Videoaufnahmen. Die Flugzeit des MD4-200 - der noch im Jahr 2008 hausintern Konkurrenz durch das deutlich größere Modell MD4-1000 erhalten soll - beträgt 15 Minuten. Dann müssen die Lithium-Ionen-Batterien ausgetauscht werden, die das Fluggerät mit Energie versorgen. Der Batterieaustausch dauert nur 1 bis 2 Minuten, bevor der Hubschrauber wieder in die Luft kann. Den Kunden wird die Abnahme von 4 Batterie-Packs empfohlen, so dass mit kurzen Unterbrechungen eine Flugzeit von rund einer Stunde möglich ist. Als optimale Flughöhe des MD4-

200 zur bestmöglichen Bilderfassung werden 25 bis 30 Meter angegeben. Rohde gibt an, dass Anfragen aus allen Bereichen der Gesellschaft vorliegen: „Behörden, Privatdetekteien oder auch Firmen, die den MD4-200 zum Personenschutz einsetzen“. Der Überlinger Wehrtechnikhersteller Diehl BGT Defence hat ein ähnliches Produkt in seinem Portfolio. Dessen „Sensor Copter“ soll eine Reichweite von bis zu 3 Kilometern haben; die Flugzeit gibt Diehl mit bis zu 30 Minuten an (www.heise.de 15.01.2008).

Gentechnik-Nachrichten

1000 Genome Project

Zwei beliebige Menschen sind zu mehr als 99% genetisch identisch. Für das verbleibende Prozent interessiert sich das „1000 Genome Project“. Es soll erklären, weshalb manche Menschen welche Krankheiten bekommen. Richard Durbin vom Wellcome Trust Sanger Institute, einer der Leiter des Konsortiums: „Für dasselbe Geld können wir heute hundertmal so viel entziffern wie früher. Das erlaubt uns, eine neue Grundlage für die Humangenetik zu legen“. Das Projekt darf zwischen 30 und 50 Mio. Dollar kosten. Wenn das Projekt voll im Gange ist, soll es in zwei Tagen mehr genetische Informationen liefern, als im ganzen Jahr 2007 in öffentliche Datenbanken gestellt wurde. Bei den 1000 ProbandInnen soll es sich um anonyme Unbekannte handeln (SZ 23.01.2008, 18).



Gentest auf Diabetes-Risiko im Online-Handel

DNA Direct vermarktet einen vom isländischen Unternehmen deCode Genetics entwickelten Test, mit dem sich überprüfen lässt, ob eine Person eine bestimmte Genvariante in sich trägt, die das Risiko für die Typ-2-Diabetes deutlich erhöht. Der Test kann für 300 US-Dollar über eine Webseite bestellt werden. Etwa 230 Mio. Menschen leiden weltweit heute unter Diabetes; für die kommenden 20 Jahre wird ein Anstieg auf 350 Mio. verausgesagt. Die Krankheit ist allerdings das Ergebnis einer komplexen Mischung aus genetischen und Umgebungsfaktoren. Neuere Studien haben mehrere Genvarianten identifiziert, die zum Auftreten der Krankheit beitragen. Diejenige mit dem offenbar größten Einfluss steckt in einem Gen mit der Bezeichnung TCF7L2: Liegt dieses einfach mutiert vor, so bedeutet dies ein leicht erhöhtes Diabetes-Risiko, zwei mutierte Gene verdoppeln die Wahrscheinlichkeit. David Altshuler, Genetiker am Broad Institute und Diabetes-Arzt in Boston/USA, würde PatientInnen den Test nicht empfehlen. Zwar scheine er korrekte Ergebnisse zu liefern; auch der Zusammenhang zwischen der Genvariation und höherem Diabetes-Risiko sei durch viele Studien belegt. Es gebe aber „keine Beweise dafür, dass der Test zu einem besseren gesundheitlichen Ergebnis führt“. Schon der Hinweis auf andere Risikofaktoren wie etwa einen überhöhten Body-Mass-Index bringe PatientInnen selten zu Veränderungen des Lebensstils. Es sei nicht zu erwarten, dass sich das durch einen Gentest ändern würde (Technology Review www.heise.de 04.12.2007).

Gentest 2.0 übers Internet

Lindsey Avey und Anne Wojcicki haben im November 2007 das Startup-Unternehmen „23andme“ gegründet, um nicht nur in den USA, sondern weltweit für 999 Dollar plus Versandkosten einen Gentest anzubieten, dessen Ergebnis dann mit Web-2.0-Techniken online visualisiert und mit anderen Daten aus der Community verknüpft werden kann. Wojcickis frisch angetrauter Ehemann, der Google-Mitgründer Sergey Brin, stellte für das Startup knapp 4 Mio. Dollar zur Verfügung und ist damit einer der größeren Investoren im Hintergrund. 23andme bezieht sich auf die 23 Chromosomen. Die Dienstleistung soll Menschen eine „Einblick in die eigenen genetischen Informationen“ bieten und setzt dabei auf „modernste DNA-Analysemethoden“. Die KundIn erhält einen „SpitKit“, einen Behälter für eine 2,5-Milliliter-Speichelprobe, die an das Vertragslabor von 23andme geschickt wird, die Firma Illumina. Dort werden 600.000 sog. SNPs (Single Nucleotide Polymophism) untersucht, die als signifikant für menschliche Unterschiede angesehen werden. 23andme leitet daraus ein „detailliertes genetisches Profil“ ab, wobei sich das Unternehmen auf eine eigens patentierte Auswahl von 30.000 SNPs mit besonders hoher Aussagekraft konzentriert.

Uta Francke, Genetik-Professorin an der US-Universität Standfort und selbst Beraterin von 23andme, relativiert: „Die SNPs haben nur eine sehr begrenzte Aussagekraft. Genaue Analysen würden das Auslesen des gesamten Erbgutes nötig machen. Bei insgesamt 3 Mrd. Basenpaaren wäre das aber derzeit mit 350.000 Dollar noch sehr teuer. Kritik wendet sich dagegen, dass die Online-Tests keine fachärztliche Betreuung und Beratung sicherstellen. Aussagen werden gemacht z.B. über Laktose-Unverträglichkeit, athletisches Potenzial und Ernährungsgewohnheiten, über das individuelle Risiko bzgl. erblichem Brust-, Darm- und Prostatakrebs, die Wahrscheinlichkeit von Diabetes oder des Nervenleidens Multiple Sklerose. Die KundInnen können dann ihre genetischen Informationen auf einer Webseite etwa 4 Wochen nach der Einsendung abrufen. Nach dem Einloggen soll mit suchmaschinenartigen Programmen im privaten Erbgut gesurft werden können. Dabei erfahren sie auch Neuigkeiten aus der Genforschung und können ihr Genom mit dem von Familienmitgliedern vergleichen, wenn diese ebenfalls teilnehmen. Ist die ganze Familie beisammen, so lässt sich der früh einsetzende Haupthaarverlust der männlichen Linie genetisch nachvollziehen. Den Eltern kann mitgeteilt werden, welcher Anteil ihres



Genmaterials in ihren Enkelkindern zu tragen kommt. Geschwister können vergleichen, wie genetisch ähnlich sie einander sind. Im Preis inbegriffen sind Updates der Suchprogramme. Avey und Wojcicki sehen einen Spaß darin, herauszufinden, dass man z.B. portugiesische Vorfahren habe. Den Einwand, dass das Wissen um eine mögliche Erkrankung die Lebensfreude beeinträchtigen können, lässt Avey nicht gelten: „Wenn die Kunden erst mal Zugriff auf ihre Daten haben, kommen sie damit sehr gut klar“, sagte sie am 22.01.2008 auf der Konferenz „Digital Life Design“ in München. Im Gegenzug sollen die Gendaten „in anonymisierter Form“ zu Forschungsinstitutionen und zur Pharmaindustrie gelangen. Das Weltwirtschaftsforum kürte das Unternehmen, hinter dem neben Google noch die Investoren Genentech und New Enterprise Associates stehen, im schweizerischen Davos zum „Technologiepionier 2008“.

Fast gleichzeitig startete das isländische Unternehmen Decode Genetics unter dem Namen deCODEme ein nahezu identisches Angebot. Konkurrent Navigenics geht mit einem „Health Compass“ für 2500 Dollar auf den Markt und gibt Informationen über „20 behandelbare medizinische Leiden“. Navigenics bietet ein Jahr lang Updates über relevante Entwicklungen in der Genforschung an, außerdem ein Informationsportal und Beratung durch einen Fachmenschen für Genetik, Der amerikanische Gentechnikpionier Craig Venter schätzt die Angebote als seriös ein und findet sie im Sinne der Aufklärung über genetische Zusammenhänge sinnvoll (vgl. DANA 4/2007, 205 f.). Die Firmen geben keine Informationen, wieviele KundInnen sie schon gewonnen haben (www.heise.de 22.01.2008; Stöcker www.spiegel.de 23.01.2008; Charisius SZ 23.01.2008, 1).

Rechtsprechung

EGMR
Journalistischer Quellenschutz gegen Erzwingungshaft

Ein niederländischer Journalist, der seine Informationsquelle nicht nennen wollte und deshalb inhaftiert wurde, hat sich mit einer Klage vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) durchgesetzt. Die Inhaftierung des Journalisten sei eine „radikalen Methode, die Personen mit genauen Informationen über Straftaten nur abschrecken können, ihre Kenntnisse der Presse weiterzuleiten“. In dem Fall ging es um Waffenhandel. Darüber hatte der Journalist ohne Nennung seiner Quellen geschrieben. Der 35jährige aus Amsterdam war im Jahr 2000 mehr als 2 Wochen lang inhaftiert worden, weil er sich geweigert hatte, seine Informationsquelle zu nennen. Drei Männer waren wegen Waffenhandels von einem Gericht verurteilt worden. „Der Quellenschutz gehört zu den Grundsätzen der Pressefreiheit“, betont das Urteil vom 22.11.2007 (Voskuil v. the Netherlands, application no. 64752/01). Der Wunsch der niederländischen Regierung, die Quelle in Erfahrung zu bringen, sei kein ausreichendes Motiv, um einen Verstoß gegen den Quellenschutz zu rechtfertigen (www.baz.ch 22.11.2007).

BVerwG
BND zur Auskunft aus Akten an Journalisten verpflichtet

Das Bundesverwaltungsgericht in Leipzig entschied mit Urteil vom 28.11.2007, dass der Bundesnachrichtendienst (BND) verpflichtet ist, dem klagenden Journalisten der Berliner Zeitung Andreas Förster Auskunft über die ihn betreffenden personenbezogenen Daten zu erteilen, auch soweit diese in Akten enthalten sind (Az. 6 A 2/07). In der Berliner Zeitung wurde ein Artikel veröffentlicht, in dem über die Observation eines Journalisten durch den BND berichtet wurde. Das Thema wurde von anderen Medien aufgegriffen. Im November 2005 beauftragte das Parlamentarische Kontrollgremium (PKG) des Deutschen Bundestags den früheren Vorsitzenden Richter am Bundesgerichtshof Dr.Gerhard Schäfer als Sachverständigen, den in der Presse erhobenen Vorwürfen nachzugehen, der BND habe über längere Zeiträume hinweg Journalisten überwacht, um so deren Informanten aus dem BND zu enttarnen. Im Mai 2006 wurde der sog. „Schäfer-Bericht“ des Sachverständigen in einer teilweise anonymisierten Fassung veröffentlicht. Förster war von 2001 bis 2005 durch eine Journalisten aus Leipzig bespitzelt worden. Schäfer bezeichnete dieses Vorgehen als rechtswidrig. BND-Präsident Ernst Uhrlau entschuldigte sich für die Aktion, auch bei Förster persönlich. Die im Mai 2006 geforderte Akteneinsicht wurde jedoch abgelehnt.

Der Kläger begehrte vom BND Auskunft über sämtliche dort gespeicherten Daten. Der BND entsprach dem Auskunftsbegehren nur hinsichtlich der elektronisch gespeicherten Daten; Auskünfte über den Inhalt seiner Akten lehnte er ab. Die hiergegen eingelegte Klage, für die das BVerwG in erster und letzter Instanz zuständig ist, hatte Erfolg. Nach § 7 S. 1 des BND-Gesetzes (BNDG) erteilt der BND Auskunft, wobei die Regelung nur von Informationen „in Dateien“ spricht. Das BVerwG stellte klar, dass im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung die Regelung verfassungskonform so ausgelegt werden muss, dass zu „gespeicherten Daten“ auch solche zählen, die in Akten enthalten sind, ohne elektronisch gespeichert zu sein. Der Ausgleich zwischen dem individualrechtlichen Auskunftsanspruch und dem nachrichtendienstlichen Geheimhaltungsinteresse wird dadurch gewährleistet, dass eine Auskunftserteilung dann unterbleibt, wenn eine Gefährdung

der Aufgabenerfüllung durch die Auskunftserteilung zu besorgen ist. Auf die gerichtliche Nachfrage hin hatte der BND ausdrücklich erklärt, dass die in § 15 Abs. 2 BVerfSchG genannten Geheimhaltungsgründe einer Auskunftserteilung an den Kläger im konkreten Fall nicht im Wege stehen. Der BND sah sich lediglich „grundsätzlich aus Rechtsgründen daran gehindert“ dem Auskunftsbegehren zu entsprechen. Der BND reagierte auf das Urteil mit der Ankündigung, er werde seine Auskunftspraxis den Vorgaben anpassen (PM BVerwG Nr. 72 v. 28.11.2007; www.heise.de 28.11.2007; www.tagesschau.de 28.11.2007).

BVerwG

Verdachtslose Abhöraktion zur Terrorismusfahndung zulässig

Am 23.01.2008 entschied das Bundesverwaltungsgericht (BVerwG) in Leipzig, dass eine strategische Überwachung des Auslandstelefonverkehrs, gegen die sich ein Betroffener zur Wehr setzte, zulässig war (Az.6 A 1.07). Bei dieser strategischen Telekommunikations- (TK-) überwachung kontrolliert der für die Auslandsaufklärung zuständige Bundes-nachrichtendienst (BND) den Telefon-, Fax- und E-Mail-Verkehr mit bestimmten Ländern. Die BND-Computer werten dabei die Kommunikation auf die Verwendung bestimmter Suchworte oder bestimmter Adressen aus. Früher vor allem mit militärischer Zielsetzung, wird die strategische TK-Überwachung seit 1994 auch gegen Terrorismus und organisierte Kriminalität eingesetzt. Ein Gremium des Bundestags genehmigt die Maßnahmen. Im Jahr 2005 waren zum Zweck der Terrorismusbekämpfung 24.427 Nachrichten ausgezeichnet worden. 83 davon wurden vom BND näher geprüft und 21 als relevant eingestuft. In einem Fall wurden die Informationen für die Sicherheit als so wichtig eingestuft, dass eine Weitergabe an die Polizei erfolgte. Das Bundesverfassungsgericht (BVerfG) hat die strategische TK-Überwachung im Jahr 1999 grundsätzlich für zulässig erklärt, obwohl hier Eingriffe zur Rede stehen, die jeden Menschen treffen können. Das BVerfG forderte allerdings, dass die Betroffenen sobald wie möglich von der Aufzeichnung unterrichtet werden müssen.



Die strategische Überwachung war nach dem 11.09.2001 angeordnet worden. Der seit 1997 in Deutschland lebende Jordanier Abu Dhess war dann Ende 2006 informiert worden, dass der BND zwischen dem 18.10 und dem 05.11.2001 fünf Nachrichten von ihm gespeichert und an das Bundeskriminalamt (BKA) weitergegeben hat. Bei einem Gespräch hatte er dem später im Irak getöteten Al-Qaida-Vorkämpfer Abu Mussab al-Sarkawi die Treue versprochen. Polizei und Verfassungsschutz überwachten ihn deshalb weiter. Mit seiner Al-Tawhid-Zelle soll er dann Anschläge in Deutschland geplant haben. Auf Grund der Aussagen eines Kronzeugen wurde er 2005 vom Oberlandesgericht Düsseldorf wegen Mitgliedschaft in einer terroristischen Vereinigung zu acht Jahren Haft verurteilt. Er beanstandete über seinen Anwalt Jens Dieckmann nun, die BND-Überwachung sei unzulässig gewesen. Der Anwalt: „Uns geht es nur um den Schutz der Grundrechte.“ Er bemängelte, dass Ende 2001 die laut Gesetz erforderliche Gefahr von Anschlägen mit „unmittelbarem Bezug“ zu Deutschland nicht bestand: „Es genügt nicht, dass der BND Informationen sammelt, die für andere Geheimdienste interessant sind“. Außerdem sei er zu spät, nämlich erst nach Jahren, über den Lauschangriff unterrichtet worden, und zudem ungenügend, in einem lapidaren Dreizeiler.

Die Aktion war dem Betroffenen nicht völlig unbekannt. Die Abhörprotokolle hatten während des Strafprozesses vorgelegen. Das BVerwG erklärte die BND-Kontrolle für rechtmäßig. Man habe damals befürchtet, dass in Deutschland sog. Schläfer, also unentdeckte Terroristen, Anschläge planten. Die Überwachung sei notwendig gewesen, um die Gefahr möglicher weiterer Anschläge „rechtzeitig zu erkennen und ihnen zu begegnen“. Die späte Information wurde akzeptiert. Allerdings sicherte der BND zu, innerhalb von vier Wochen Nummern und genauen Zeitpunkt der Telefonate mitzuteilen (Rath www.taz.de 24.01.2008; www.tagesschau.de 24.01.2008; Ramelsberger SZ 25.01.2008, 1, 6).

BGH

Hamburger Postbeschlagnahme rechtswidrig

Mit Beschluss vom 28.11.2007 erklärte der Ermittlungsrichter des Bundesgerichtshofes (BGH) die Art und Weise einer im Frühjahr 2007 vorgenommenen Postbeschlagnahme im Wesentlichen für rechtswidrig. Im Mai 2007 hatten Beamte des Bundeskriminalamtes (BKA) auf Grund eines Brandanschlags auf das Auto des Bild-Chefredakteurs Kai Diekmann gegen Mitglieder der linksextremen „militanten gruppe“ (mg) ermittelt. Bei der Suche nach Bekennerschreiben kontrollierten 16 Fahnder eigenhändig tausende Sendungen des hamburger Briefzentrums 20, ob sie bestimmten Rasterkriterien entsprechen. Die Aktion wurde später erfolglos eingestellt. Der BGH-Richter stellte nun fest, dass das Aussortieren von Postsendungen allein Aufgabe der Postbediensteten ist. „Eine Mitwirkung von Ermittlungsbeamten oder auch des Richters“ sei dagegen „grundsätzlich ausgeschlossen“, um die „Vertraulichkeit des übrigen Postverkehrs nicht zu gefährden“. Die Angestellten müssten verdächtige Briefe der Staatsanwaltschaft oder dem Richter aushändigen. Gegen die Postdurchsuchung in Hamburg hatte sich ein Anwalt beschwert (Az. 1 BGs 519/2007). Die verantwortliche Bundesanwaltschaft erklärte, sie nehme die Entscheidung zur Kenntnis. Die Beanstandung habe aber keine weiteren Konsequenzen.

Die Entscheidung hat nach Ansicht des stellv. Vorsitzenden der Humanistischen Union, Fredrik Roggan, auf weitere Ermittlungsverfahren Auswirkungen, z.B. auf die kurz zuvor erfolgte Sichtung von Schreiben an vier Berliner Zeitungsredaktionen. Auch dort hatten Polizeibeamte beim Sortieren der Postsendungen „geholfen“. Roggan widersprach damit einer Stellungnahme



von Justizstaatssekretär Lutz Diwell, der auf eine parlamentarische Anfrage des grünen Bundestagsabgeordneten Hans-Christian Ströbele erklärte, die Bundesregierung sehe „keinen Anlass für Konsequenzen aus den Vorgängen“. Diwell verteidigte die Kontrollaktion in Berlin, keinesfalls seien sämtliche Absender an die vier Berliner Zeitungen „festgestellt“ worden: „Es erfolgte keinerlei Erfassung der in Augenschein genommenen Postsendungen“. Vielmehr seien die zwei letztlich beschlagnahmten Briefe anhand von Kriterien wie dem Fehlen eines Absenders ausgesondert worden. Es sei dann zur Sicherheit eine dem Grundsatz der Verhältnismäßigkeit geschuldete „Gegenlicht-Kontrolle“ mit einer starken Lichtquelle durchgeführt worden. Die „Einschaltung von Polizeibeamten“ in den „Sortiervorgang“ diente nur der „Beschleunigung der Maßnahme“. Zudem sollte gemäß Diwell damit sichergestellt werden, „dass sich die Ausleitung von Briefen“ von vornherein „auf das zwingend erforderliche Maß beschränkt“.



Für die Postbeschlagnahme setzt die Strafprozessordnung (StPO) grds. keine besonders hohen Hürden. Im Fall von Hamburg wie von Berlin ging es aber auch um das Ausspionieren von Briefen an Berufsgeheimnisträger wie Anwälte und Journalisten, die einen besonderen Schutz genießen. Um die gesuchten Briefe an die Zeitungen auszusortieren, mussten alle an die Blätter gerichteten Schreiben zumindest von außen in Augenschein genommen werden Im Berliner Fall konnte die Polizei an den zwei Tagen der Maßnahme so komplett registrieren, wer an die Redaktion Briefe gesandt hatte (Krempl www.heise.de 28.11.2007; SZ 01./02.12.2007, 8; www.spiegel.de 30.11.2007).

BGH
Keine vorbeugende Unterlassungsklage gegen Bildveröffentlichungen

Die bekannte 29jährige frühere Schwimmsportlerin Franziska van Almsick scheiterte mit ihrem Versuch, die Veröffentlichung von Fotos in mehreren von den beklagten Verlagen Burda und Bauer-Verlagsgruppe herausgegebenen Zeitschriften (Viel Spaß, Neue Woche, Freizeitwoche) präventiv zu verbieten. Fotos waren während eines Ferienaufenthaltes im Jahr 2005 auf Sardinien heimlich angefertigt worden und zeigen die Klägerin und ihren Partner Jürgen Harder u.a. am Strand vor dem Hotel. Die mit den Fotos bebilderten Artikel waren überschrieben mit dem Namen der Klägerin und ihres Partners und trugen Untertitel wie „Turtelnd und verliebt im Urlaub“. Die beklagten Verlage hatten auf das Unterlassungsbegehren der Klägerin jeweils vorgerichtlich in strafbewehrten Unterlassungsverpflichtungen erklärt, dass sie es unterlassen werden, die bereits veröffentlichten Fotos erneut zu verbreiten. Van Almsick gab sich hiermit aber nicht zufrieden und beantragte in zwei Verfahren, generell die Verbreitung von Bildnissen von ihr, die sie in ihrem privaten Alltag zeigen, zu verbieten. Die Vorinstanz des Kammergerichtes Berlin hatte im Berufungsverfahren diesen Antrag für zu weitgehend erachtet, aber die Verlage verurteilt, es zu unterlassen, im Kern gleichartige Bilder wie die vorgerichtlich beanstandeten zu veröffentlichen. Doch selbst diese Auslegung ging dem zuletzt so prominentenfreundlichen Bundesgerichtshof (BGH) zu weit, der das Berliner Urteil aufhob.

Auf die Revision wies der für das allgemeine Persönlichkeitsrecht zuständige VI. Zivilsenat des BGH beide Klagen in vollem Umfang zurück. Die Rechtswidrigkeit der bereits erfolgten Veröffentlichungen stehe im Hinblick auf die vorgerichtlich abgegebenen Unterlassungsverpflichtungen nicht im Streit. Ob der Klägerin ein Anspruch auf die Unterlassung der Veröffentlichung „kerngleicher“ Bilder zustehe, könne nicht im Voraus beurteilt werden. Für die Zulässigkeit einer Bildveröffentlichung sei in jedem Einzelfall eine Abwägung zwischen dem Informationsinteresse der Öffentlichkeit und dem Interesse des Abgebildeten an dem Schutz seiner Privatsphäre erforderlich. Eine solche Interessenabwägung könne nicht in Bezug auf Bilder vorgenommen werden, die noch gar nicht bekannt sind und bei denen insbesondere offen ist, in welchem Kontext sie veröffentlicht würden. Bei der gebotenen Abwägung könnte auch die begleitende Wortberichterstattung eine wesentliche Rolle spielen (BGH U.v. 13.11.2007, VI ZR 265/06 u. VI ZR 269/06; BGH PE 170/2007 v. 13.11.2007; Kerscher SZ 14.11.2007, 17).

OLG Köln
Lehrer müssen öffentliche Internetbenotung hinnehmen

Das Oberlandesgericht (OLG) Köln hat die Benotung von LehrerInnen im Internet in einem einstweiligen Rechtsschutzverfahren in zweiter Instanz mit Beschluss vom 27.11.2007 für rechtmäßig und damit das Vorurteil des Landgerichtes (LG) für zutreffend erklärt (15 U 142/07). Geklagt hatte eine Gymnasiallehrerin, die von SchülerInnen im Internetforum Spickmich.de mit einer Gesamtnote von 4,3 bewertet worden war. Das Schülernetzwerk wird von drei Kölner Studenten betrieben und versteht sich als „Ort für Meinungsäußerungen und den Austausch von Schülern untereinander“. Gemäß eigenen Angaben sind dort über 150.000 einzelne Lehrernoten hinterlegt. SchülerInnen können Bewertungen in Form von Schulnoten zu verschiedenen Kategorien abgeben, etwa zu „fachlich kompetent“, „gut vorbereitet“, faire Noten“, aber auch „sexy“, „cool und witzig“, „menschlich“ oder „beliebt“. Die Benotungsdienst hat über 150.000 angemeldete Benutzerinnen.

Die Lehrerin aus dem niederrheinischen Neunkirchen-Vluyn fühlte sich durch die Benotungen mehrerer SchülerInnen verunglimpft und in ihrem Persönlichkeitsrecht verletzt. Zuvor hatte das LG Köln den Antrag gegen die Veröffentlichung ihres Namens und der von ihr unterrichteten Fächer für zulässig erklärt. Sie müsste eine Benotung hinnehmen, solange keine diffamierende Schmähkritik geäußert werde. Das OLG stellte fest, dass „das Forum prinzipiell dem Schutzbereich des Grundrechts auf Meinungsfreiheit gemäß Artikel 5 Abs. 1 des Grundgesetzes unterfalle, wobei das Grundrecht aber nicht schrankenlos

gelte und seine Grenze in den allgemeinen Gesetzen und im Recht der persönlichen Ehre finde". Nach Aussagen des Vorsitzenden des 15. Zivilsenates des OLG, Axel Jährig, muss im Hauptsacheverfahren noch geklärt werden, inwieweit die Lehrerbewertung durch Außenstehende manipuliert werden könne. Insgesamt werde die Bedeutung der Benotung möglicherweise überschätzt. Eine Entscheidung durch den Bundesgerichtshof als Revisioninstanz oder durch das Bundesverfassungsgericht halte er in der Sache für durchaus hilfreich. Zwar habe Spickmich.de teilweise eine konkreten Sachbezug zum Unterricht. Betroffen sei aber auch die Persönlichkeit der jeweiligen Lehrkraft in ihren individuellen Ausprägungen: „Die Frage, ob Lehrer in die Öffentlichkeit gezogen werden dürfen, ist sehr ernsthaft zu stellen und darf nicht ins Ulkige gezogen werden". Eine Bewertung unter den genannten Kriterien könne „durchaus der Orientierung von Schülern und Eltern dienen und zu einer wünschenswerten Kommunikation, Interaktion und erhöhten Transparenz führen." Das Gericht bekräftigte, dass auch Meinungen, die lediglich unter einer E-Mail-Adresse oder auch anonym im Internet abgegeben würden, den Schutz der Meinungsfreiheit genießen. Ob Kriterien wie „sexy" oder „hässlich" die Grenze zur Schmähkritik überschreiten, ließ das Gericht offen, weil die Betreiber diese Rubriken inzwischen entfernt hatten.



Der Initiator von Spickmich.de, Tino Keller, erklärte, die juristische Beurteilung der Lehrerbenotung stärke die inhaltliche Position des Webangebots. Dies sei in Deutschland überfällig gewesen: „Wir achten auf Fairness. Beleidigungen haben bei uns keinen Platz und sind auch von den Schülern nicht gewollt". Kurz vorher zu Beginn des Schuljahres 2007/2008 hatte die Schulministerin von Nordrhein-Westfalen Barbara Sommer (CDU) angekündigt, Internetseiten, auf denen Lehrkräfte diskriminiert würden, durch die Bezirksregierung sperren zu lassen. Sie richtete eine Beschwerdestelle für PädagogInnen ein, die sich durch ihre SchülerInnen gemobbt fühlten. Justizministerin Roswitha Müller-Piepenkötter (CDU) ermunterte die Lehrkräfte, die sich von ihren Schülern im Internet beleidigt sähen, Strafanzeige zu stellen. Der Vorsitzende des Philologenverbands Heinz-Peter Meidinger kritisierte das Urteil scharf: „Der Datenschutz wird bei Lehrern offenbar weniger ernst genommen als bei Normalbürgern". Er empfahl LehrerInnen, die Zustimmung zur Veröffentlichung persönlicher Daten im Internet zurückzuziehen. Die „öffentliche Bloßstellung der Lehrer" in den manipulationsanfälligen Internetportalen zeige, dass es den Initiatoren vor allem um Aufmerksamkeit und Werbeeinnahmen gehe. Die Gewerkschaft Erziehung und Wissenschaft (GEW) betonte, das Internet sei ein menschlich und pädagogisch ungeeigneter Ort für eine Lehrerbewertung. Josef Kraus, Präsident des Deutschen Lehrerverbands, appellierte an die Vernunft der SchülerInnen und Eltern, bei Problemen über einen Vertrauenslehrer das Gespräch zu suchen.

Am 30.01.2008 entschied das LG Köln erneut gegen die Lehrerin und für das Schülerportal. Es wies die Klage im Hauptsacheverfahren als unzulässig zurück: „Durch die Bewertungen sind nicht das Erscheinungsbild oder die allgemeine Persönlichkeit der Klägerin betroffen, sondern die konkrete Ausübung ihrer beruflichen Tätigkeit." Die Lehrerin will gegen das Urteil Berufung einlegen. Nach Aussage ihrer Anwältin strebt sie eine Grundsatzentscheidung beim Bundesgerichtshof oder beim Bundesverfassungsgericht an. Die Datenschutzaufsichtsbehörde von Bayern, die Regierung von Mittelfranken erklärte trotz der Rechts-prechung, sie halte die Internet-Plattform Spickmich.de für nicht zulässig. Das Recht der Lehrer auf informationelle Selbstbestimmung habe mehr Gewicht als das Grundrecht der Mein ungsäußerungsfreiheit. Behörden-leiter Günther Dorn: „Die Zur-Schau-Stellungen und Anprangerungen im Internet sind für die Lehrer in vielen Fällen schwerwiegend" (www.heise.de 06.11.2007; SZ 07.11.2007, 7; Nitschmann SZ 08.11.2007, 13; www.heise.de 27.11.2007; Taffertshofer SZ 28.11.2007, 1; www.heise.de 23.01.2008, 28.01.2008, 30.01.2008).

VG Berlin

Telekommunikationsanbieter haben Entschädigungsanspruch für TK-Überwachungs-Hard- und -Software

Das Verwaltungsgericht (VG) Berlin hat in einem Beschluss von Anfang November 2007 angemahnt, dass im Fall des umstrittenen Abhörens von Auslandsverbindungen eine staatliche Entschädigung bereits für Investitionen in die erforderliche Aufrüstung der Überwachungsinfrastruktur fällig ist. Andernfalls würden Geschäftskundenanbieter gemäß den bestehenden Regelungen über Ausgleichszahlungen leer ausgehen. Der juristische Kampf des Mitglieds der „Initiative Europäischer Netzanbieter" (IEN) zieht sich bereits eine Weile hin. Dem IEN gehören Konzerne wie BT, Cable&Wireless, Colt Telecom, Tiscali oder Verssatel an. Vor mehr als einem Jahr hatte das TK-Unternehmen das Bundesverfassungsgericht (BVerfG) angerufen. Es sollte direkt klären, ob und in welchem Umfang die Unternehmen für ihre Zuarbeiten bei der Bespitzelung ihrer KundInnen angemessen zu entschädigen sind. Das BVerfG verwies aber die Firma zunächst an die niederen Instanzen

Das VG Berlin hat nun in einem Verfahren des vorbeugenden Rechtsschutzes festgestellt, dass der Auslandskopf-Überwachung erhebliche verfassungsrechtliche Bedenken entgegenstehen. Der Antrag des klagenden Unternehmens zur Aussetzung der Überwachungsverpflichtung richtet sich gegen die Bestimmungen zur Verschärfung der Telekommunikations-Überwachungsverordnung (TKÜV), wonach Anbieter von Auslandsverbindungen auch Telefonate und E-Mail abhörbar machen müssen, die über die deutschen Grenzen hinaus vermittelt werden. Seit Anfang 2007 müssen die Betreiber von sog. Auslandsköpfen gemäß der TKÜV den bereits abhörbaren Sprachverkehr noch einmal an der „Grenzübertrittstelle" der Netzknoten ins Ausland an die



Sicherheitsbehörden übermitteln. Ziel ist es, die Kommunikation zu erfassen, bei der nur der ausländische Anschluss bekannt ist. Die betroffenen Firmen sind dem IEN zufolge durch die

Regelung zu weiteren Millionen-investitionen gezwungen. Dabei sei auch der Bundesregierung klar, dass die verpflichteten Telcos „in keiner Beziehung zu möglichen Tätern stehen und für die anfallenden Daten bei den Behörden kein Bedarf nachgewiesen wurde".

Die 27. Kammer des VG untersagte es der zuständigen Bundesnetzagentur als Vertreterin des Bundeswirtschaftsministeriums, vor dem rechtskräftigen Abschluss im anhängigen Hauptsacheverfahren Ordnungsmaßnahmen gegen die Antragstellerin einzuleiten. Die klagende Firma ist damit vorläufig nicht gezwungen, Einrichtungen zur Umsetzung des Auslandskopf-Überwachung vorzuhalten: „Eine Inanspruchnahme Privater für staatliche Aufgaben wurde schon in vorkonstitutioneller Zeit als jedenfalls entschädigungspflichtige Aufopferung verstanden." Selbst dann, wenn dem Verpflichteten eine staatlich abzuwendende Störung zurechenbar sei, stehe die Belastung des Verpflichteten mit den entstehenden Kosten auch unter der „Prämisse der Zumutbarkeit". Das VG hält es für nötig, den Fall jetzt dem BVerfG vorzulegen. Bis zu weiteren Klärungen muss die Antragstellerin die Überwachungstechnik nicht auf eigene Kosten einrichten und bereithalten, da diese auf Grund nicht ersichtlicher Schadensersatzansprüche auch bei einem Obsiegen im Hauptsacheverfahren nicht erstattet würden. Dem gegenüber würden die Nachteile für die Ermittler bei einer Aussetzung der Auslandskopf-Überwachung durch das Unternehmen „eher gering" erscheinen. Diese solle ohnehin nicht „lückenlos" erfolgen.



Für die Rechtmäßigkeit der erweiterten Überwachungsbestimmung genügt es nach Ansicht des VG nicht, dass der Bundesnetzagentur bei der Verhängung von Bußgeldern ein Ermessensspielraum eingeräumt ist. Vergleichbar mit der aktuell beschlossenen Vorratsdatenspeicherung sind die betroffenen Firmen verpflichtet, die Überwachungspflichten umgehend umzusetzen. Dies, so das VG, gelte selbst dann, wenn wie vorliegend nicht nachgewiesen sei, dass in der Praxis überhaupt ein Bedürfnis der Behörden für die Investition bei Geschäftskundenanbietern besteht. IEN-Geschäftsführer Jan Mönikes: „Damit wird das gesamte Konstrukt der Vorratsdatenspeicherung und der geplanten Entschädigungsverordnung erschüttert." Falls keine Ausgleichsmaßnahmen auch für Investitionen in Hard- und Software für TK-Überwachungsmaßnahmen vorgesehen werden, würde voraussichtlich die gesamte Regelung kippen. Mönikes kündigte an, zumindest auf eine Härteregelung zur Entschädigung von Investitionskosten zu pochen. Andernfalls würde die IEN mit ihren Mitgliedern auch die Vorratsdatenspeicherung auf ihre Verfassungsgemäßheit hin überprüfen lassen (Krempl www.heise.de 06.12.2007).

VG Köln

Verfassungsschutz darf Linken-Politiker Ramelow nicht beobachten

Das Verwaltungsgericht (VG) Köln hat am 17.01.2008 in einem Feststellungsurteil entschieden, dass das Bundesamt für Verfassungsschutz (BfV) den Vize-Fraktionschef der Linken im Bundestag Bodo Ramelow nicht überwachen darf (Az. 20 K 3077/06). Dies gilt für seine Zeit als Landtagsabgeordneter in Thüringen und als Mitglied des Bundestags. Das BfV hatte zuvor erklärt, nur „öffentlich zugängliche Informationen" gesammelt zu haben. Das Gericht betonte, es handele sich nicht um eine grundsätzliche Entscheidung darüber, ob der Verfassungsschutz Informationen über Landtags- und Bundestagsabgeordnete sammeln dürfe. Auch wurde nicht grundsätzlich darüber entschieden, ob der Inlandsgeheimdienst die Partei „Die Linke" beobachten darf. Es sei nur um den Einzelfall Ramelow gegangen. Das Gericht hatte in Bezug auf den Kläger seinen Status als Abgeordneter, seine Parteifunktionen und seine konkrete politische Betätigung gewürdigt. Nach dieser Prüfung lägen die gesetzlichen Voraussetzungen für eine Beobachtung nicht vor. In einem zweiten Verfahren unterlag der 51jährige Politiker. Er wollte auch ein Auskunftsrecht zu allen über ihn gespeicherten Daten erstreiten. Soweit Ramelow ihn betreffende Auskünfte aus Personenakten Dritter oder Sachakten fordere, sei die Klage unzulässig, weil der Kläger zuvor das BfV um Auskunft hätte bitten müssen. Aber auch in der Sache sah das Gericht keine Verpflichtung des BfV (Az. 20 K 6242/03).

Ramelow nannte das Urteil einen „Sieg des Rechtsstaates, denn gegen das Ministerium für Staatssicherheit hätte ich mich so nie zur Wehr setzen können". Das BfV habe eine „totale Schlappe" erfahren. Die Maßstäbe, die das Gericht an ihn persönlich angelegt habe, würden für Fraktionskollegen wie Gregor Gysi oder Bundesgeschäftsführer Dietmar Bartsch gelten, über die ebenfalls Dossiers angelegt wurden. Die „verschrobene Argumentation der Geheimdienste ist komplett zerstört worden". Die Linksfraktion hat im Sommer 2007 auch eine Klage beim Bundesverfassungsgericht gegen ihre nachrichtendienstliche Beobachtung eingereicht. Sie dürfe nicht weiter „mit geheimdienstlichem Dreck diskreditiert werden und der Verfassungsschutz muss erkennen, dass der kalte Krieg beendet ist", so Ramelow. Kurz zuvor hat das Saarland als erstes westdeutsches Bundesland bekannt gegeben, die Beobachtung der Linken eingestellt zu haben. Er gebe keine Anhaltspunkte mehr für ein verfassungsfeindliches Wirken der Partei. Von den 53 ParlamentarierInnen überwacht das BfV Ramelow zufolge 16 Abgeordnete. Nach dem Urteil bezweifelte der Präsident des BfV, ob eine Überwachung der Linkspartei noch nötig sei. Die Grundsatzpapiere der Linken enthielten zwar Hinweise auf das Ziel, das politische System zu überwinden: „Man muss dennoch immer fragen, ob es noch verhältnismäßig ist, die Linke zu beobachten". Insofern bedürfe es einer Abstimmung mit dem Bundesinnenministerium. Der SPD-Innenexperte Dieter Wiefelspütz erklärte, er halte eine generelle Beobachtung der Linkspartei durch

den Verfassungsschutz nicht für angebracht (www.spiegel.de 17.01.2008; www.tagesschau.de 17.01.2008; Graalmann SZ 18.01.2008, 4, 6; SZ 28.01.2008, 6)

LG München I

Selbstjustiz gegen illegale Videoüberwachung unzulässig

Ein zu Unrecht per Videoüberwachung Gefilmter darf nicht zur Selbstjustiz greifen und die eingesetzte Kameraausrüstung zerstören. Dies entschied das Landgericht (LG) München im Fall einer illegalen Kamerabeobachtung durch einen Wohnungsbesitzer, Mitglied einer Eigentümergemeinschaft, der mehrfach bestohlen worden war und deshalb in der gemeinsamen Tiefgarage ein Kamera anbrachte, mit deren Hilfe er die Straftäter dingfest machen wollte. Doch statt dessen wurde das elektronische Gerät von einem Unbekannten zerstört. Der Wohnungsbesitzer reparierte die erste Kamera und installierte zur besseren Überwachung eine weitere. Über diese war zwei Jahre später ein Nachbar bei der Zerstörung der ersten Kamera zu erkennen. Der Geschädigte forderte Schadenersatz. Das LG entschied, dass der Täter den Schaden ersetzen muss, den er nachweisbar angerichtet hatte. Selbst wenn das Filmen nicht erlaubt gewesen sei, habe er nicht auf diese Weise überreagieren dürfen. Die weiteren geltend gemachten Kosten - für die Zerstörung der ersten Kamera und die Montage der zweiten Kamera - erhielt der Kläger nicht ersetzt. Beides sei, so das Gericht, dem Nachbarn nicht anzulasten (LG München I B. v. 22.12.2006; Az. 13 S 12178/06; Schleswig-Holstein Ztg. 21.01.2008, Ratgeber S. 1; PM Amtsgericht München 5.3.2007).



Bundesverfassungsgericht

Kein Datenschutz bei Abtretung von Darlehensforderungen

Nach dem Bundesgerichtshof (BGH) musste sich nun auch das Bundesverfassungsgericht (BVerfG) mit der Frage befassen, ob das Bankgeheimnis oder das Bundesdatenschutzgesetz der Abtretung von Darlehensforderungen an Inkasso-unternehmen entgegenstehen. Der BGH hatte diese Frage im Februar 2007 verneint (siehe Bericht in DANA 2/2007). Die Kläger hatten daraufhin Verfassungsbeschwerde vor dem BVerfG erhoben.

Das BVerfG nahm die Beschwerde mangels Erfolgsaussichten nicht zur Entscheidung an. Das Gericht begründete seinen Beschluss damit, dass die Bank gemäß § 402 des Bürgerlichen Gesetzbuchs verpflichtet sei, dem Inkassounternehmen die zur Geltendmachung der Forderung notwendigen Auskünfte zu erteilen und die erforderlichen Unterlagen zu übergeben. Diese gesetzliche Regelung begegne keinen verfassungsrechtlichen Bedenken. Eine Abwägung zwischen dem Geheimhaltungsinteressen des Schuldners und dem Interesse an der Verkehrsfähigkeit der Forderung sei vom Gesetz nicht vorgesehen und auch nicht von Verfassungs wegen geboten. Ein Abtretungsverbot könne jedoch möglicherweise dann bestehen, wenn die Darlehensunterlagen besonders sensible Informationen enthielten. Dann sei es Aufgabe der Zivilgerichte, dem Recht des Schuldners auf informationelle Selbstbestimmung bei der Urteilsfindung Rechnung zu tragen. Auf welche Art dies geschehen soll, ließ das BVerfG offen, weil es für die vorliegende Verfassungsbeschwerde ohne Belang war (Bundesverfassungsgericht, Beschluss vom 11.07.2007, Az. 1 BvR 1023/07, Wertpapier-Mitteilungen 36/2007, S. 1594).

OVG Bremen

Private Dateien auch auf Dienst-PC geschützt

Private Dateien eines Beamten sind auch dann besonders geschützt, wenn sie auf einem Dienst-PC gespeichert sind. Sie dürfen durch den Dienstherrn nur auf Grundlage einer richterlichen An-ordnung geöffnet und gesichtet werden. Dies stellte das Oberverwaltungsgericht (OVG) Bremen im Fall eines Polizeikommissars fest, gegen den wegen des Verdacht der Unterschlagung von Verwarnungsgeldern strafrechtlich und disziplinarisch ermittelt wurde. Im Zuge der Strafermittlungen wurde auch der Dienst-PC des Polizeibeamten untersucht. Dabei stießen die Ermittler in einem Dateiordner namens „Strafanzeigen" auf insgesamt vierzig Dateien mit sexistisch-pornografischen Inhalt. Dieser Zufallsfund führte zu einem Disziplinarverfahren gegen den Polizisten.

Der Beamte erhob Klage und hatte damit in zweiter Instanz vor dem OVG Bremen Erfolg. Das Gericht hob die Beschlagnahme der vierzig Dateien auf. Die Durchsuchung, so das OVG, sei rechtswidrig gewesen, da sie ohne richterliche Anordnung ergangen war. Eine solche sei aber gemäß § 102 der Strafprozessordnung und § 27 des Bremer Disziplinargesetzes erforderlich gewesen. Daran ändere auch die Tatsache nichts, dass der Polizeibeamte die Dateien auf seinem Dienst-PC gespeichert habe. Entscheidend seien nicht die Eigentumsverhältnisse, sondern die Frage, wer die Sachherrschaft über den Rechner und die Dateien gehabt habe. Dies sei der Beamte gewesen, der den Dienst-PC mit einem Kennwort geschützt hatte, das nur ihm bekannt war.

Das OVG bewegte sich mit dieser Entscheidung auf einer Linie mit dem Landgericht Bremen. Das Landgericht hatte den Fall aus strafprozessualer Sicht zu beurteilen und war dabei ebenfalls zu der Auffassung gelangt, dass die Durchsuchung mangels richter-licher Anordnung rechtswidrig war (Oberverwaltungsgericht Bremen, Beschluss vom 21.07.2006, Az. DL A 420/05, Zeitschrift für Beamtenrecht 11/2007, S. 394).

BVerfG

Genetischer Fingerabdruck eines jugendlichen Ersttäters

Ist jemand verdächtigt, eine Straftat von erheblicher Bedeutung oder eine Sexualdelikt begangen zu haben, so dürfen ihm Körperzellen entnommen und molekulargenetisch untersucht werden.



Dieser „Genetische Fingerabdruck" soll dazu dienen, in künftigen Strafverfahren die Identität des Täters zu klären. Voraussetzung ist jedoch, dass Grund zu der Annahme besteht, dass der Beschuldigte auch künftig Straftaten von erheblicher Bedeutung begehen wird (so § 81 g Strafprozessordnung).

Das Bundesverfassungsgericht hatte bereits im Jahr 2000 festgestellt, dass diese Regelung verfassungskonform ist. Allerdings muss die Gerichtsentscheidung, die einen solchen tiefgreifenden Eingriff in das informationelle Selbstbestimmungsrecht anordnet, „tragfähig begründet" sein. Ihr muss eine „zureichende Sachaufklärung, insbesondere durch Beiziehung der verfügbaren Straf- und Vollstreckungsakten, des Bewährungshefts und zeitnaher Auskünfte aus dem Bundeszentralregister" vorausgehen. In den Ent-scheidungsgründen müssen alle bedeutsamen Umstände abgewogen werden. „Dabei ist stets eine auf den Einzelfall bezogene Entscheidung erforderlich; die bloße Wiedergabe des Gesetzeswortlauts reicht nicht aus" (BVerfG, Beschluss vom 14.12.2000, 2 BvR 1741/99, BVerfGE 103, 21).



Sieben Jahre nach dieser Entscheidung musste das Bundesverfassungsgericht feststellen, dass sich offenbar nicht alle Instanzgerichte an diese Rechtsprechung gebunden fühlen: Ein zur Tatzeit fünfzehnjähriger Schüler war vom Jugendgericht wegen einer Prügelei unter Gleichaltrigen zu Freizeitarrest und gemeinnütziger Arbeit verurteilt worden. Nach der Verurteilung verpflichtete ihn das Amtsgericht, seinen genetischen Fingerabdruck abzugeben, da bei ihm die Gefahr eines Rückfalls bestehe. Zur Begründung bezog sich das Amtsgericht u. a. auf die „strafrechtlichen Vorbelastungen" des Jugendlichen. Allerdings hatte der Amtsrichter schlampig gearbeitet: Der Schüler war strafrechtlich zuvor noch gar nicht in Erscheinung getreten. Zudem hatte er sich nach der Tat bei seinem Opfer entschuldigt und einhundert Stunden für gemeinnützige Zwecke gearbeitet. Das Jugendgericht hatte deshalb eine Wiederholungsgefahr verneint. Dies war dem Amtsrichter jedoch auf Grund seiner „nachlässig fehlerhafte[n] Sachaufklärung" (Zitat BVerfG) unbekannt geblieben. Das Bundesverfassungsgericht bezweifelte auch, dass eine Schulhofprügelei als „Straftat von erheblicher Bedeutung" anzusehen ist. Es hob deshalb den Beschluss des Amtsgerichts wegen Verstoßes gegen das Recht auf informationelle Selbstbestimmung auf.

Die Hilfsbegründung des Amtsgericht, der genetische Fingerabdruck könne ja auch der Entlastung des Jugendlichen in späteren Strafverfahren dienen, ließ das Bundesverfassungsgericht übrigens nicht gelten: „Die Inanspruchnahme einer Person, die voraussichtlich keine Straftaten begehen wird, wird im Übrigen auch nicht dadurch gerechtfertigt, dass die Feststellung und Speicherung des DNA-Identifizierungsmusters gegebenenfalls als Entlastungsbeweis dienen könnte" (BVerfG, Beschluss vom 18.09.2007, 2 BvR 2577/06, NJW 2008, 281).

Buchbesprechungen



Peter Gola, Georg Wronka
Handbuch zum Arbeitnehmer-datenschutz
Datakontext, Frechen, 2008, 4. überarbeitete und erweiterte Auflage
ISBN 3-89577-450-9; EUR 78

(ks) Das Handbuch zum Arbeitnehmerdatenschutz gehört seit Jahren zum unverzichtbaren Arbeitsmittel für Betriebsräte, Datenschutzbeauftragte und alle, zu deren Aufgaben die datenschutzgerechte Gestaltung des Umgangs mit Arbeitnehmerdaten gehört. Eine Überarbeitung wurde jedoch seit längerem schmerzlich vermisst, weil das Werk trotz einer Neuauflage von 2004 etwas „in die Jahre gekommen" war. Sowohl die Novellierung des BDSG 2006 als auch wesentliche technische und betriebliche Entwicklungen hatten bisher keinen Eingang in das Werk gefunden.

Bei Durchsicht der neuen Ausgabe fällt zunächst auf, dass die grundlegende Struktur des Werkes, nämlich die Orientierung an den durch das BDSG definierten Verarbeitungsphasen im wesentlichen beibehalten wurde. Lediglich der bereits früher separat bearbeiteten Frage des Verhältnisses von Datenschutz und Mitbestimmung sind, neben den allgemein einleitenden Kapiteln, auch hier wieder zwei eigene Kapitel gewidmet. Die phasenorientierte Sicht verhindert leider an vielen Stellen eine praxisfreundlichere Darstellung betriebsprozessual gemeinsam zu betrachtender Fragestellungen.

Auch verwirren die uneinheitlich verwendeten Begriffe. So wird „Personaldaten" unzutreffend und ohne weitere Definition teilweise als Synonym für personenbezogene Arbeitnehmerdaten verwendet (z. B. wenn im 7. Kapitel unter „Das Verändern und Nutzen von Peronaldaten" auch offensichtlich nicht unter Personaldaten zu fassende Daten subsumiert werden). Andere Verarbeitungsphasen beziehen sich dann nur noch ganz allgemein auf Daten (z. B. im 9. Kapitel „Das Löschen, Berichtigen und Sperren von Daten"). Hier würde man sich etwas mehr Sorgfalt und Präzision dringend wünschen.

Das neu eingefügte und etwas missverständlich überschriebene Kapitel 6 „Datenerhebung und –speicherung durch technische Kontrollen" sammelt Fragestellungen, die sich außerhalb der Datenverarbeitung durch die Personalabteilung ergeben.

Missverständlich deshalb, weil es hierbei nicht nur um Kontrollen geht, sondern auch um die unzähligen Applikationen, deren Funktionalität zwar Kontrollmöglichkeiten einschließt (und die daher mitbestimmungspflichtig sind), die jedoch vorrangig meist einem anderen Zweck dienen.

Insgesamt hätte man sich bei der Aufarbeitung sowohl neuer Technologien als auch bekannter Fragstellungen wesentlich mehr Ergänzungen und Überarbeitungen gewünscht. Ausführungen über Blackberry, RFID und Location Based Services beispielsweise bleiben an der Oberfläche und streifen die in der betrieblichen Praxis regelmäßig zu klärenden datenschutzrechtlichen Fragen nur. Wer in seinem Betrieb mit einem umfassenden Flottenmanagement-System zu tun bekommt, wird den Hinweis wenig hilfreich finden, dass die Zulässigkeit von Handy-Ortung durch den Arbeitgeber möglicherweise vom Interesse an Senkung von Verwaltungsaufwand gedeckt sein kann.

Dass die phasenorientierte Betrachtung dem Verständnis einzelner Fragestellungen recht abträglich sein kann, wird beispielsweise bei den neu aufgenommenen Betrachtungen zum Whistleblowing deutlich: Das Verfahren wird im Kapitel über das Erheben und Speichern von Peronaldaten dargestellt. Ein vager Hinweis auf Zugriffsrechte findet sich im Kapitel „Transparenzpflichten“. Den mit der Gestaltung eines datenschutzgerechten Whistleblowing-Systems verbundenen Fragestellungen wird dies nicht gerecht. Welch Datenschutz-Anforderungen sind an ein solches System und das zugehörige Berechtigungskonzept zu stellen? Wer darf den Namen des Whistleblowers überhaupt erfahren? Für wen ist es erforderlich? Wann müssen welche Daten des Melders und des Angezeigten gelöscht werden? Wann muss der Angezeigte informiert werden? Dies alles wird nicht thematisiert.

Viele datenschutzrelevante Themen, die im heutigen betrieblichen Alltag großes Gewicht gewonnen haben, sucht man zu dem vergebens, wie beispielsweise Betrachtungen zu forensischen Analysen. Die großen Vorzüge des Werks liegen nach wie vor in den umfassenden Verweisen auf die aktuelle Rechtsprechung und die detaillierte Darstellung der Schnittstelle zwischen Datenschutz und Mitbestimmung. Allein aus diesem Grunde ist das Werk immer noch unentbehrlich für die eingangs erwähnten Nutzergruppen, auch wenn die Erwartungen durch die vorliegende Ausgabe leider nur teilweise erfüllt wurden. Es bleibt zu wünschen, dass die Autoren mit der nächsten Neuauflage eine inhaltliche Neustrukturierung verbinden.



Peter Schaar:
„Das Ende der Privatsphäre“
Paperback, 256 Seiten, 12,5 x 20,5 cm, ISBN: 978-3-570-00993-2, € 14,95

Wenn der amtierende Bundesdatenschutzbeauftragte zur Feder greift, um ein Buch über „Das Ende der Privatsphäre“ zu verfassen, muss es schlimm um den Datenschutz bestellt sein. Aber schon die Unterzeile des Werks – „Der Weg in die Überwachungs gesellschaft“ – relativiert den alarmistischen Titel ein wenig. Wer auf dem Weg ist, der ist offenbar noch nicht am Ziel angekommen. Und wenn es nach Peter Schaar geht, dürfen wir dieses Ziel eines Gesellschaftssystems ohne Privatsphäre und Datenschutz auch nie erreichen.

Schaars Werk ist in fünf Teile gegliedert. In den drei mittleren schildert er, wie Technik, Staat und Wirtschaft unsere Privatheit bedrohen. Als Kenner der Materie hakt Schaar routiniert alle bedeutenden Punkte der derzeitigen Datenschutzdiskussion ab: RFID, Ubiquitous Computing, Videoüberwachung, Biometrie, Online-Durchsuchung, Vorratsdatenspeicherung, Fluggastdaten und Scoring – um nur einige zu nennen. Dabei bleibt Schaar sachlich, fast distanziert. Seine kritischen Beschreibungen treffen zwar stets den Kern des jeweiligen Problems, sie berühren den Leser jedoch nicht. Stellenweise hat man das Gefühl, eine Kurzfassung des letzten BfD-Tätigkeitsberichts in den Hände zu halten. Engagierter und persönlicher wird Schaar jeweils zum Beginn und zum Ende des Buches. Er spart dabei nicht mit Appellen und Lösungsvorschlägen, fordert eine Reform des Datenschutzrechts und datenschutzfreundliche Technologien. Beides soll auf einer „Ethik der Informationsgesellschaft“ basieren. Die grundlegenden, existenziellen Probleme des Datenschutzes geht Schaar aber nicht an – die Fragen, warum so viele Menschen keinen Wert auf ihre Privatsphäre legen und wie man diesem Zustand abhelfen kann.

Nach gut zweihundertfünfzig Seiten legt der fachkundige Leser das flüssig geschriebene, gut verständliche Buch mit einem gewissen Bedauern aus der Hand. Schaar bleibt an der Oberfläche, ist mehr Chronist und Analytiker denn Missionar, beschreibt nur bereits bekannte Missstände und Gefahren. Neue Rezepte hat auch er nicht anzubieten. Dies ist kein Vorwurf, vielleicht gibt es keine besseren Lösungen als die dargestellten. Die Datenschutzdiskussion in Fachkreisen wird durch Schaars Werk jedoch nicht neu angeregt werden.

Trotzdem ist „Das Ende der Privatsphäre“ eine empfehlenswerte Lektüre. Zielgruppe sind diejenigen, die sich – ohne Experten zu sein – für den Datenschutz und seine fortlaufende Einschränkung interessieren. Für sie bietet Schaars Werk zu einem moderaten Preis einen umfassenden und aktuellen Ein- und Überblick in das Thema. Von daher ist dem Buch eine möglichst große Leserschaft zu wünschen.





Urteil zum Kfz-Massenabgleich muss Folgen haben

Pressemitteilung der Beschwerdeführer vom 11.03.2008:

Das Bundesverfassungsgericht hat am heutigen Dienstag den heimlichen und verdachtslosen Abgleich von Kfz-Kennzeichen mit polizeilichen Fahndungsdateien für verfassungswidrig erklärt. Die Beschwerdeführer begrüßen das Urteil und fordern auch von den nicht unmittelbar betroffenen Bundesländern (Bayern, Bremen, Hamburg, Mecklenburg-Vorpommern, Rheinland-Pfalz) die Abschaffung ihrer entsprechenden, zu weit gehenden Ermächtigungen. Darüber hinaus bedeutet das Urteil nach unserer Überzeugung das endgültige Aus für Pläne, an Flughäfen oder Bahnhöfen beliebige Menschen unter Verwendung biometrischer oder anderer Verfahren mit Fahndungsdateien abzugleichen oder zu orten.



Dem heutigen Urteil des Bundesverfassungsgerichts zufolge sind die Vorschriften über den Kfz-Massenabgleich zu unbestimmt und gehen unverhältnismäßig weit. Anders als von den Ländern gewollt, darf der massenhafte Abgleich von Nummerschildern nicht ohne besonderen Anlass routinemäßig vorgenommen werden. Wörtlich heißt es in dem Urteil: “Die automatisierte Erfassung von Kraftfahrzeugkennzeichen darf nicht anlasslos erfolgen oder flächendeckend durchgeführt werden. Der Grundsatz der Verhältnismäßigkeit im engeren Sinne ist im Übrigen nicht gewahrt, wenn die gesetzliche Ermächtigung die automatisierte Erfassung und Auswertung von Kraftfahrzeugkennzeichen ermöglicht, ohne dass konkrete Gefahrenlagen oder allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder –verletzungen einen Anlass zur Einrichtung der Kennzeichenerfassung geben.”

Als einer der erfolgreichen Beschwerdeführer gibt der Datenschutzexperte und Bürgerrechtler Roland Schäfer zu bedenken: “Die vorliegende Entscheidung korrigiert nur eine der zahlreichen überzogenen gesetzlichen Eingriffsbefugnisse. Andere Befugnisse werden nicht oder nicht erfolgreich vor den Verfassungsgerichten angefochten. Es ist daher dringend geboten, dass sich Bürger vermehrt zusammenschließen, um auch auf der politischen Ebene diesen machthungrigen Staat in seine Grenzen zu verweisen.”

Der Jurist Patrick Breyer, der den schleswig-holsteinischen Landtag vergeblich vor der Einführung des verfassungswidrigen Kfz-Massenabgleichs gewarnt hatte, erklärt: “Das heutige Urteil ist ein Armutszeugnis für die Landesregierungen von CDU, CSU und SPD, denen die Unvereinbarkeit dieser Regelung mit unserer Verfassung bekannt sein musste. Wir brauchen Verbesserungen des Gesetzgebungsverfahrens, um die Besorgnis erregende Zunahme verfassungswidriger Gesetze zu bremsen.”

Die dem heutigen Urteil zugrunde liegenden Verfassungsbeschwerden richteten sich gegen das hessische und das schleswig-holsteinische Polizeigesetz, die beide den zügellosen Einsatz automatischer Kennzeichenlesegeräte erlaubten, um Fahrzeuge zu melden, nach denen gefahndet wird. Der automatisierte Kfz-Kennzeichenmassenabgleich erfolgte heimlich und ohne Anlass. Ein solches massenhaftes Stochern im Nebel behandelt jeden Autofahrer wie einen potenziellen Straftäter und legt den Grundstein für einen immer umfangreicheren maschinellen Abgleich der Bevölkerung mit polizeilichen Datenbanken. Konkrete mit den Geräten erzielte Erfolge waren kaum zu vermelden. Auch wenn die Polizei versichert, sie habe kein Interesse an den Daten der Verkehrsteilnehmer, für die keine Fahndungsnotierung vorliegt, so werden zunächst doch alle Verkehrsteilnehmer durchgesiebt. Allein durch die Möglichkeit automatischer Verkehrsüberwachung wird psychischer Druck erzeugt, der geeignet ist, die allgemeine Handlungs- und Bewegungsfreiheit zu beschränken.

Der Kfz-Kennzeichenmassenabgleich stellt im Kern einen Präzedenzfall einer allgemeinen, heimlichen und anlasslosen Überwachung der Bevölkerung dar. Wäre eine generelle, verdachtslose Kennzeichenüberwachung zugelassen worden, wäre der Überwachung der gesamten Bevölkerung durch permanenten Abgleich mit allen polizeilichen Fahndungsdateien Tür und Tor eröffnet worden. Solchen Überwachungsvorhaben hat das Bundesverfassungsgericht einen Riegel vorgeschoben und damit unseren Freiheitsrechten erneut einen großen Dienst erwiesen.

Alle drei Beschwerdeführer wurden durch den Freiburger Datenschutzexperten und Rechtsanwalt Dr. Kauß vertreten.



2007

1 **Steuerhinterziehungserklärung**

Eingangsstempel

2 Steuernummer

3 Ich bin doch nicht besteuert

200713568521

Allgemeine Angaben

4 Steuerflüchtige Person

Veranlagung — Veranlagungsschlüssel: schwerkriminell = sk, mittelkriminell = mk, eigentlich ganz nett = egn

5 Vor- oder Deckname

6 Konzernchef von

Religion — Religionsschlüssel: römisch-katholisch = rk, evangelisch = ev, bin selbst Gott = bsg

7 Anzahl der Aufsichtsratsposten (nur angeben, wenn mehr als 5, sonst Pauschbetrag)

Steuerlicher Wohnsitz

8 X Liechtenstein | X Guernsey | X Macao | X Kann mir den Namen nicht merken | X tagsüber erreichbar

9 X Cayman Islands | X Jersey | X Punica-Oase | X bisher unerreicht

10 Zurzeit flüchtig im Raum:

Fremdwährungen, in die ich investiert habe:

11 X Cayman-Dollar | X Miles & More | X Tengelmann-Treueherzen

Angaben zur Hinterziehung

12 Hiermit bezichtige ich mich, den folgenden Betrag nicht ordnungsgemäß versteuert zu haben: Betrag (in Mio. EUR) (falls Platz nicht ausreicht, bitte gesondertes Blatt verwenden)

13 Stattdessen habe ich das Geld: X in Steuerparadiese transferiert | X in Scheinfirmen reinvestiert | X meinem Hund überschrieben | X in Stiftungen gesteckt

14 Falls in Zeile 13 angegeben: Meine Stiftung trägt folgenden Namen: X irgendwas Lateinisches | X An-Stiftung | X wie mein Hund

Grund der Steuerhinterziehung:

15 X Ich bin doch nicht blöd | X Geiz ist geil

Werbungskosten

16 Koffer EUR ,- | Mövenpick-Macaos EUR ,-

17 Steuerschlupflocher von Leitz ,- | Abo manager magazin ,-

Dienstfahrzeuge

18 Porsche Cayman EUR ,- | Steuerflüchtlingsboot EUR ,-

Pendlerpauschale

19 bitte Strecke ankreuzen: X Bonn–Liechtenstein | X Davos–St. Moritz | X Mechthild–Julia

Anlagen

20 X Anlage Geliebte (CIC) | X Ferienanlage (MALEDIVEN)

21 X Anlage Spenden (SCHMIER) | X das weiß nur mein Anlageberater

Bitte freilassen. Vom Finanzbeamten auszufüllen:

- den knöpft sich der Chef selbst vor
- direkt nach Bochum leiten
- beide Augen ganz fest zudrücken

22 Bei meiner Verhaftung sollten folgende Medien anwesend sein:

X Ich stimme ich einer Verwertung meiner Daten als DVD zu.

Unterschrift

23 Datum, Unterschrift(en)

Hiermit versichere ich, dass mein Steuerberater bei der Erstellung der Steuerhinterziehungserklärung nicht mitgewirkt hat.

